

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW MEXICO**

UNITED STATES OF AMERICA,

Plaintiff,

vs.

No. CR 13-1876 JB

JASON LOERA,

Defendant.

**MEMORANDUM OPINION AND ORDER**

**THIS MATTER** comes before the Court on the Defendant's Motion to Suppress Evidence, filed March 7, 2014 (Doc. 35) ("Motion"). The Court held an evidentiary hearing on May 20, 2014, and May 21, 2014. The Court heard the parties' arguments on the Motion on August 19, 2014. The primary issues are: (i) whether Defendant Jason Loera may seek suppression of the child pornography found on Loera's laptop computer and compact discs ("CDs"); (ii) whether the Search and Seizure Warrant, issued November 19, 2012, submitted to the Court at the May 20, 2014, evidentiary hearing as Government's Hearing Exhibit 9 ("First Warrant"), satisfies the particularity requirement in the Fourth Amendment to the Constitution of the United States of America; (iii) whether Federal Bureau of Investigation ("FBI") Special Agent Aaron Cravens' and Special Agent Brian Nishida's on-site preview of Loera's CDs during the execution of the First Warrant on November 20, 2012, was within the First Warrant's scope; (iv) whether the agents conducted an unlawful search when they continued searching Loera's CDs for evidence of computer fraud and electronic mail hijacking after they discovered child pornography; (v) whether the agents acted in good faith when they continued to search for evidence of computer fraud and electronic mail hijacking after discovering child pornography;

(vi) whether Cravens was permitted to open files on Loera's CDs on November 27, 2012, for the limited purpose of providing a United States Magistrate Judge a description of four images depicting the sexual abuse of a child; (vii) whether, even if Cravens was not permitted to open the files on November 27, 2012, and even if those descriptions are excised from the affidavit in support of the Second Warrant, probable cause to issue the Search and Seizure Warrant (issued November 29, 2012), submitted to the Court at the May 20, 2014, evidentiary hearing as Government's Hearing Exhibit 10 ("Second Warrant") still exists; (viii) whether, even if the Second Warrant suffered from an incurable defect, Nishida relied on that warrant in good faith when he searched Loera's CDs and laptop for child pornography; and (ix) whether, even if the Second Warrant contained an incurable defect and Nishida did not execute the Second Warrant in good faith, the agents inevitably would have discovered child pornography.

The Court will deny the Motion. The Court concludes that Loera may seek suppression of the child pornography evidence, because he admitted that the CDs and laptop on which the agents discovered child pornography were within his control and possession when the agents seized them. The Court holds that the First Warrant satisfies the particularity requirement in the Fourth Amendment, because it limited the agents' search to evidence of computer fraud and electronic mail hijacking. The Court concludes that the agents' on-site preview of Loera's CDs during the execution of the First Warrant on November 20, 2012, was within the warrant's scope, because the warrant authorized the agents to open image and video files, and files with last-modified and created dates before July 29, 2011. The Court further holds that, while the Court is concerned with the soundness of the United States Court of Appeals for the Tenth Circuit's law related to computer searches, under that law, which the Court, as a district court, must faithfully apply, the agents conducted an unlawful search when they continued searching for evidence of

electronic mail hijacking and computer fraud on Loera's CDs after they discovered child pornography. The Court concludes, however, that the agents acted in good faith when they did so. The Court holds that Cravens was not permitted to open files on Loera's CDs on November 27, 2012, for the limited purpose of providing a United States Magistrate Judge a description of four images depicting the sexual abuse of a child. The Court concludes, however, that, even if Cravens was not permitted to open the files on November 27, 2012, and even if those descriptions are excised from the Affidavit in Support of an Application Under Rule 41 for a Warrant to Search and Seize (issued November 29, 2014), submitted to the Court at the May 20, 2014, evidentiary hearing as Government's Hearing Exhibit 9 ("Second Affidavit"), probable cause to issue the Second Warrant still existed. The Court holds that, even if the Second Warrant suffered from an incurable defect, Nishida relied on that warrant in good faith when he searched Loera's CDs and laptop for child pornography. Finally, the Court holds that, even if the Second Warrant contained an incurable defect and Nishida did not execute the second warrant in good faith, the agents inevitably would have discovered child pornography on Loera's CDs and laptop. Accordingly, the Court will deny the Motion, and not exclude the child pornography evidence from the trial.

### **FACTUAL BACKGROUND**

Rule 12(d) of the Federal Rules of Criminal Procedure requires the Court to state its essential findings on the record when deciding a motion that involves factual issues. See Fed. R. Crim. P. 12(d) ("When factual issues are involved in deciding a motion, the court must state its essential findings on the record."). This Memorandum Opinion and Order's findings of fact shall serve as the Court's essential findings for rule 12(d) purposes. The Court makes these findings under the authority of rule 104(a) of the Federal Rules of Evidence, which requires a judge to

decide preliminary questions relating to the admissibility of evidence, including the legality of a search or seizure, and the voluntariness of an individual's confession or consent to search. See United States v. Merritt, 695 F.2d 1263, 1269-70 (10th Cir. 1982)(“[U]nder Rule[] 104(a) . . . , the district court ‘is not bound by the Rules of Evidence except those with respect to privilege.’”)(quoting United States v. Matlock, 415 U.S. 164, 174 (1974)). In deciding such preliminary questions, the other rules of evidence, except those with respect to privileges, do not bind the Court. See Fed. R. Evid. 104(a) (“The court must decide any preliminary question about whether a witness is qualified, a privilege exists, or evidence is admissible. In so deciding, the court is not bound by evidence rules, except those on privilege.”). Thus, the Court may consider hearsay in ruling on a motion to suppress. See United States v. Merritt, 695 F.2d at 1269 (“The purpose of the suppression hearing was, of course, to determine preliminarily the admissibility of certain evidence allegedly obtained in violation of defendant's rights under the Fourth and Fifth Amendments. In this type of hearing the judge had latitude to receive it, notwithstanding the hearsay rule.”); United States v. Garcia, 324 F. App'x 705, 708 (10th Cir. 2009)(unpublished)(“We need not resolve whether Crawford [v. Washington], 541 U.S. 36 (2004)]’s<sup>1</sup> protection of an accused's Sixth Amendment confrontation right applies to suppression hearings, because even if we were to assume this protection does apply, we would conclude that the district court's error cannot be adjudged ‘plain.’”);<sup>2</sup> United States v. Ramirez,

---

<sup>1</sup>Crawford v. Washington stands for the proposition that testimonial out-of-court statements against an accused are inadmissible at trial unless the witness is unable to testify and the defendant had a previous opportunity to cross examine the witness. See 541 U.S. at 53-54.

<sup>2</sup>United States v. Garcia is an unpublished opinion, but the Court can rely on an unpublished opinion to the extent its reasoned analysis is persuasive in the case before it. See 10th Cir. R. 32.1(A), 28 U.S.C. (“Unpublished opinions are not precedential, but may be cited for their persuasive value.”). The Tenth Circuit has stated:

388 F. App'x 807, 810 (10th Cir. 2010)(unpublished)("It is beyond reasonable debate that Ramirez's counsel were not ineffective in failing to make a Confrontation Clause challenge to the use of the confidential informant. The Supreme Court has not yet indicated whether the Confrontation Clause applies to hearsay statements made in suppression hearings."). Cf. United States v. Hernandez, 778 F. Supp. 2d 1211, 1226 (D.N.M. 2011)(Browning, J.)(concluding "that Crawford v. Washington does not apply to detention hearings").<sup>3</sup>

# **1. The November 20, 2012 Searches.**

1. On November 19, 2012, United States agents applied for a search warrant for

---

In this circuit, unpublished orders are not binding precedent, . . . and we have generally determined that citation to unpublished opinions is not favored. However, if an unpublished opinion or order has persuasive value with respect to a material issue in a case and would assist the court in its disposition, we allow a citation to that decision.

United States v. Austin, 426 F.3d 1266 (10th Cir. 2005). The Court finds that United States v. Garcia, United States v. Ramirez, 388 F. App'x 807 (10th Cir. 2010)(unpublished), and United States v. Reed, 195 F. App'x 815 (10th Cir. 2006)(unpublished), have persuasive value with respect to material issues, and will assist the Court in its disposition of this Memorandum Opinion and Order.

<sup>3</sup>Loera does not object under Crawford v. Washington to any evidence in this case; the Court, therefore, need not decide whether Crawford v. Washington applies to suppression hearings. The Court notes, however, that the courts that have decided whether the Confrontation Clause applies to suppression hearings have found that Crawford v. Washington does not apply to suppression hearings. See Ebert v. Gaetz, 610 F.3d 404, 414 (7th Cir. 2010)(Tinder, J., joined by Posner, & Rovner, JJ.)(holding the right of confrontation does not apply at a suppression hearing); United States v. Garcia, 324 F. App'x 705, 708 (10th Cir. 2009)(unpublished)("There is no binding precedent from the Supreme Court or this court concerning whether Crawford applies to pretrial suppression hearings. To the extent that we can divine clues from our case law concerning the resolution of this issue, they do not benefit Mr. Garcia."). Cf. United States v. Morgan, 505 F.3d 332, 339 (5th Cir. 2007)("[W]e hold that Crawford v. Washington does not apply to the foundational evidence authenticating business records in preliminary determinations of the admissibility of evidence."); United States v. Saneaux, 365 F. Supp. 2d 493, 498 n.5 (S.D.N.Y. 2005)(concluding that Crawford v. Washington does not apply to determining whether a statement is admissible under the coconspirators hearsay exception: "[B]ecause the Court is not bound by the Rules of Evidence in the disposition of preliminary matters such as this one, I may properly consider such evidence even if it cannot be introduced at trial.").

Loera's residence, seeking evidence that Loera committed computer fraud and hijacked electronic mail transmissions. See Application for Search Warrant at 1 (issued November 19, 2012), submitted to the Court at the May 20, 2014, evidentiary hearing as Government's Hearing Exhibit 9 ("First Application").

2. The United States filed an affidavit in support of the First Application. See Affidavit in Support of an Application Under Rule 41 for a Warrant to Search and Seize (issued November 19, 2014), submitted to the Court at the May 20, 2014, evidentiary hearing as Government's Hearing Exhibit 9 ("First Affidavit").

3. The First Affidavit alleges that Loera possessed electronic mail transmissions intended for New Mexico Governor Susana Martinez and her staff that had been sent through Martinez' gubernatorial campaign website, [www.susana2010.com](http://www.susana2010.com) ("the Domain"). See First Affidavit ¶ 28 at 10.

4. The First Affidavit states that one of Martinez' supporters created the Domain on July 18, 2009, and registered the website for two years with the website hosting company GoDaddy.com ("GoDaddy"). See First Affidavit ¶ 5, at 2.

5. According to the First Affidavit, during the 2010 gubernatorial campaign, Martinez and her staff used the Domain to, among other purposes, communicate with each other and individuals outside of the campaign through electronic mail transmissions. See First Affidavit ¶ 6, at 2-3.

6. The First Affidavit alleges that only the individual or individuals who had the Domain's username and password could renew the Domain when it expired in July, 2011. See First Affidavit ¶ 7, at 3.

7. According to the First Affidavit, Jamie Estrada maintained the username and

password for the Domain during Martinez' 2010 gubernatorial campaign. See First Affidavit ¶ 8, at 3.

8. According to the First Affidavit, at some point before the election, Martinez discovered Estrada reading her electronic mail transmissions and removed him from the campaign. See First Affidavit ¶ 8, at 3.

9. The First Affidavit reports that, after Martinez was elected governor in November, 2010, Martinez and her staff continued to use the electronic mail accounts linked to the Domain. See First Affidavit ¶ 10, at 4.

10. The First Affidavit alleges that, on or about July 18, 2011, however, Martinez' staff began receiving reports that electronic mail transmissions sent to their Domain addresses were not being delivered. See First Affidavit ¶ 10, at 4.

11. The First Affidavit states that Martinez' staff determined that the electronic mail transmissions were not being delivered, because the Domain had expired. See First Affidavit ¶ 10, at 4.

12. According to the First Affidavit, Martinez' staff tried to re-register the Domain, but none of the staff had the Domain's username and password. See First Affidavit ¶ 11, at 4.

13. The First Affidavit states that Martinez' staff contacted Estrada for the username and password, but Estrada refused to provide the information. See First Affidavit ¶ 12, at 4.

14. According to the First Affidavit, due to Estrada's refusal to provide the username and password, Martinez' staff could not re-register the Domain. See First Affidavit ¶ 12, at 4.

15. The First Affidavit asserts that, after unsuccessfully attempting to re-register the Domain, Martinez and her staff transitioned to a new domain, [www.susanapac.com](http://www.susanapac.com). See First Affidavit ¶ 13, at 4.

16. The First Affidavit states that, after this transition, Martinez and her staff believed that the Domain had expired and was no longer in use. See First Affidavit ¶ 13, at 5.

17. According to the First Affidavit, in or about June, 2012, local media outlets obtained and published an electronic mail transmission that was sent to Martinez' Domain electronic mail account on or about May 2, 2012. See First Affidavit ¶ 14, at 5.

18. According to the First Affidavit, the release of this electronic mail transmission prompted Martinez and her staff "to believe that the Domain had not in fact expired, but was still being used by someone unaffiliated with Martinez's organization." First Affidavit ¶ 14, at 5.

19. The First Affidavit stated that, whoever re-registered the Domain was redirecting electronic mail transmissions to "another account unassociated with the Domain." First Affidavit ¶ 14, at 5.

20. According to the First Affidavit, the United States learned that the Domain expired on July 18, 2011, that it had a forty-two day grace period thereafter, and that, on July 29, 2011, a GoDaddy account that listed "Sylvia Tacori" as the accountholder re-registered the Domain. See First Affidavit ¶¶ 16-17, at 6.

21. The First Affidavit stated that the address for the Tacori account belonged to a Chipotle restaurant. See First Affidavit ¶ 18, at 6.

22. The First Affidavit asserted that the United States could not identify anyone living in the United States with the name Sylvia Tacori. See First Affidavit ¶ 18, at 6.

23. The First Affidavit stated that, based in part on this information, the United States concluded that the Tacori account was "fictitious." First Affidavit ¶ 18, at 6.

24. According to the First Affidavit, the Tacori account was created with a cellular telephone assigned to Estrada. See First Affidavit ¶ 20, at 7.



25. The First Affidavit states that, two days after the July 29, 2011, re-registration of the Domain, Estrada's telephone logged into the Tacori account. See First Affidavit ¶ 20, at 7.

26. According to the First Affidavit, the United States learned of a July 15, 2012, electronic mail transmission from the electronic mail address OMMARRAVENHERST@GMAIL.COM ("OMAR") that contained information from Martinez' electronic mail account at the Domain. See First Affidavit ¶ 21, at 7-8.

27. The First Affidavit states that, based in part on this information, the United States received a search warrant for the OMAR account. See First Affidavit ¶ 22, at 8.

28. According to the First Affidavit, the execution of the OMAR search warrant "confirmed that the [OMAR] account did in fact contain numerous emails that were intended for Governor Martinez and her staff during the period of time the Domain is believed to have been comprised by the subject(s)." First Affidavit ¶ 23, at 8.

29. According to the First Affidavit, the United States discovered "several emails sent from the OMAR account to JASONLOERA@GMAIL.COM [("JASONLOERA")]. . . which included . . . emails intended for Governor Martinez and/or her staff." First Affidavit ¶ 26, at 9.

30. The First Affidavit alleges that the JASONLOERA account is registered to Loera and "is regularly accessed from the . . . same IP address used to access the OMAR account." First Affidavit ¶ 27, at 9-10.

31. The First Affidavit alleges that the IP address used to access the JASONLOERA and OMAR accounts is associated with Loera's residence. See First Affidavit ¶ 27, at 10.

32. Consequently, on November 19, 2012, FBI Special Agent Michael Boady secured a warrant to search Loera's residence. See First Warrant at 1.

33. The First Warrant incorporated by reference Attachment B to the First

Application (“Attachment B”). See First Warrant at 1.

34. Under “identify the person or describe the property to be searched and give its location,” the First Warrant states: “See Attachment B to affidavit in support of application, incorporated herein by reference.” First Warrant at 1.

35. Under “[t]he person or property to be searched, described above, is believed to conceal,” the First Warrant states: “See Attachment B to affidavit in support of application, incorporated herein by reference.” First Warrant at 1.

36. Attachment B details the scope of the First Warrant as follows:

1. All records, in any form, relating to violations of Title 18 U.S.C. § 2511 (Interception and disclosure of wire, oral, or electronic communications prohibited) and Title 18 U.S.C. § 1030 (Fraud and related activity in connection with Computers), involving Jason Loera or others including:
  - a. Usernames, passwords, and other account information for email accounts, Google Apps accounts, domain accounts, accounts for credit, debit, or gift cards, and online storage accounts;
  - b. Records which are related to the use of computer programs to re-direct email from one domain to another;
  - c. All records and/or communications related to the susana2010.com and susanapac.com domains or the intrusion thereof;
  - d. All bank records, checks, credit or debit card bills, account information, and other financial records from June 2011 to the present.
  - e. Records relating to the provision of internet and phone service;
  - f. Records showing the technical or computer knowledge.
2. Any computers, cell phones, and/or electronic media that could have been used as a means to commit the offenses described on the warrant.
3. For any computers, cell phones, tablets, computer hard drives, or other physical objects upon which computer data can be recorded/stored

(hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in the warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
  - c. evidence of the counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
  - d. evidence of the times the COMPUTER was used;
  - e. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
  - f. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
  - g. contextual information necessary to understand the evidence described in this attachment.
4. Records and things evidencing the use of computers and/or the internet to commit the fraud activity described in the Search Warrant Affidavit, including:
- a. Routers, modems, and network equipment used to connect computers to the Internet;
  - b. Records of Internet Protocol addresses used;
  - c. Records of wireless internet connections
  - d. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever forms and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

5. Any and all statements for bank accounts, which include transactions from June 1, 2011 to the present.
6. Any and all documents, printouts, hand written statements, electronic communications, and in whatever form related to the following:
  - a. The Susana2010.com domain
  - b. Communications with GoDaddy.com and DomainsByProxy.com
  - c. The SusanaPAC.com domain
  - d. The interception of emails related to the Susana2010.com Domain.
7. Any and all records in whatever form related to email accounts maintained, controlled or used in any manner by Jason Loera.

Attachment B ¶¶ 1-7, at 2-5.

37. On November 20, 2012, FBI agents -- including Cravens and Nishida -- executed the First Warrant at Loera’s residence. See Transcript of Evidentiary Hearing at 52:9-17 (taken May 20, 2014)(“May 20, 2014 Tr.”)(Cravens, Tuckman).

38. Cravens and Nishida understood that the purpose of the search was to find and seize evidence of electronic mail hijacking and computer fraud. See May 20, 2014 Tr. at 53:7-11 (Cravens, Tuckman); id. at 152:6-8 (Nishida, Tuckman); id. at 160:5-11 (Nishida, Tuckman).<sup>4</sup>

---

<sup>4</sup>Loera contends that, on November 14, 2014, Boady, the Special Agent in charge of Loera’s case, told Nishida to search a laptop that was seized from Loera’s residence for evidence of child pornography on November 20, 2014. See May 20, 2014 Tr. at 22:2-24 (Serna). In support of this contention, Loera cites a passage of a report in which Nishida detailed his examination of Loera’s laptop computer and the computer’s hard drive. See Report of Examination at 1 (dated February 28, 2013), submitted to the Court at the May 20, 2014,

39. The FBI agents discovered a large volume of electronic media in Loera's residence -- including CDs, DVDs, laptop computers, external hard drives, a USB flash drive,<sup>5</sup> an iPhone, and an iPad. See May 20, 2014 Tr. at 154:22-155:1 (Nishida, Tuckman).

40. Cravens and Nishida were responsible for "previewing" the CDs at Loera's residence to determine if they contained evidence of electronic mail hijacking or computer fraud. See May 20, 2014 Tr. at 57:23-58:6 (Cravens, Tuckman); id. at 153:14-154:6 (Nishida, Tuckman).

41. The purpose of previewing the CDs was to ensure that the FBI seized only CDs that contained information relevant to the investigation. See May 20, 2014 Tr. at 57:24-58:6

---

evidentiary hearing as Government Exhibit 13 ("Feb. 28, 2013 Examination Report"). The passage states: "On November 14, 2012, SA Michael Boady requested that the above listed specimen(s) be examined for evidence of 'Intercepting a Communication,' e.g.,] e-mail messages to/from the domain 'Susana2010.com.' In addition, SA Boady requested that the evidence also be examined for evidence of Child Pornography (CP) possession and receipt." Feb. 28, 2013, Examination Report at 1.

Loera's point seems to be that Nishida was simultaneously conducting two searches when he executed the First Warrant on November 20, 2014: one for evidence of the unlawful interception of electronic communications and computer fraud pursuant to the First Warrant, and another for child pornography. This argument is unpersuasive for a few reasons. First, because Boady had already gone through the trouble of obtaining the First Warrant, it would be illogical for him to not include a request to search for child pornography in the First Warrant if he had any reason to believe the search would uncover it. Second, Nishida testified that he wrote this passage to summarize all of Boady's requests regarding the Dell laptop and the eighty-gigabyte hard drive -- it was not intended to indicate that Boady had requested Nishida to search the items on November 14, 2012. See May 20, 2014 Tr. at 201:11-20 (Nishida, Serna); id. at 202:16-24 (Nishida, Serna). Third, both Cravens and Nishida testified multiple times that the purpose of the November 20, 2012, search was to uncover evidence of the unlawful interception of electronic communications and computer fraud, and not child pornography. See May 20, 2014 Tr. at 53:7-11 (Cravens, Tuckman); id. at 152:6-8 (Nishida, Tuckman); id. at 160:5-11 (Nishida, Tuckman). The Court has no reason to question their uncontroverted testimony.

<sup>5</sup>A USB flash drive is a "data storage device that includes flash memory with an integrated Universal Serial Bus interface. USB flash drives are typically removable and rewritable, and physically much smaller than a [compact disc]. Most weigh less than . . . 1.1oz." "USB Flash Drive," Wikipedia.org, [http://en.wikipedia.org/wiki/USB\\_flash\\_drive](http://en.wikipedia.org/wiki/USB_flash_drive) (last visited Oct. 10, 2014).

(Cravens, Tuckman); id. at 68:23-69:11 (Cravens, Tuckman); id. at 155:8-24 (Nishida, Tuckman).

42. Cravens and Nishida split up the CDs between themselves and searched them separately. See May 20, 2014 Tr. at 119:2-14 (Cravens, Serna).

43. Cravens initially tried to view the files on the CDs using a program called FTK Imager. See May 20, 2014 Tr. at 58:18-22 (Cravens).

44. FTK Imager can be used to limit a CD or hard drive search to a particular type of file -- i.e., to search for only image, text, or audio files. See May 20, 2014 Tr. at 101:5-11 (Cravens, Serna).

45. When Cravens attempted to use the FTK Imager software on the first CD that he found, however, it showed that the CD was empty. See May 20, 2014 Tr. at 103:1-3 (Cravens, Serna).

46. Assuming that the FTK Imager software was malfunctioning, Cravens closed the software and opened the CD on his Windows desktop, which showed that the CD was not empty, but instead contained a number of files. See May 20, 2014 Tr. at 58:18-25 (Cravens, Tuckman).

47. Cravens used the “thumbnail view” to preview the files -- meaning that he saw small images of the files, the file names, and the file types. May 20, 2014 Tr. at 59:1-8 (Cravens, Tuckman).

48. Cravens “tr[ie]d to use the thumbnails” to determine if the files contained relevant evidence, and he “clicked on anything that didn’t appear correct, or any documents.” May 20, 2014 Tr. at 92:6-11 (Cravens).

49. Although he tried to use the thumbnails to identify which CDs contained relevant evidence, Cravens believed that the First Warrant authorized him and Nishida “to go through the

entire contents of the CDs.” May 20, 2014 Tr. at 92:9-11 (Cravens).

50. Cravens seized only CDs that contained “documents related to the Domain” and anything “that might have been evidence of domain e-mail hijacking.” May 20, 2014 Tr. at 68:18-22 (Cravens).

51. While Cravens was “scrolling down through the images or files . . . on the CDs, [he] found what looked like a nude child, and opened” up the file. May 20, 2014 Tr. at 60:5-7 (Cravens).

52. Cravens stated that, based on the thumbnail view, “it appeared to be a child pornography image,” but he “enlarge[d] it to confirm” that it was. May 20, 2014 Tr. at 139:12-17 (Cravens, Court).

53. Cravens viewed the first child pornography image for “under 30 seconds.” May 20, 2014 Tr. at 61:6-12 (Cravens, Tuckman).

54. After Cravens found the first child pornography image, he ejected the CD containing the image from his computer and set it aside. See May 20, 2014 Tr. at 61:12-13 (Cravens).

55. Cravens did not write down a filename or description of the first image. See May 20, 2014 Tr. at 61:24-25 (Cravens, Tuckman).

56. After finding the first child pornography image, Cravens did not seek advice from an Assistant United States Attorney, a colleague, or a supervisor, whether he should obtain a search warrant for child pornography. See May 20, 2014 Tr. at 115:16-25 (Cravens, Serna).

57. Instead, Cravens told Boady -- the FBI special agent in charge of Loera’s case -- and Nishida that he had found child pornography, and continued to search for evidence of electronic mail hijacking and computer fraud. See May 20, 2014 Tr. at 65:15-17 (Cravens,

Tuckman); id. at 116:3-12 (Cravens, Serna); id. at 158:25-159:1 (Nishida, Tuckman).

58. Although he was not searching for more child pornography images after finding the first one, Cravens thought he might find more child pornography on Loera's CDs. See May 20, 2014 Tr. at 65:10-17 (Cravens, Tuckman); id. at 66:1-4 (Cravens, Tuckman).

59. Cravens later found a child pornography image on a second CD. See May 20, 2014 Tr. at 67:18-68:4 (Cravens, Tuckman).

60. As he had done with the first CD, Cravens immediately set the CD aside and did not open any other files on that CD. See May 20, 2014 Tr. at 67:21-23 (Cravens, Tuckman).

61. Although he was searching for evidence of electronic mail hijacking or computer fraud, Cravens opened files that appeared to be images, because they "could have been a picture of a person or personal information, identifying information, or . . . a screen shot<sup>6</sup> of e-mail or domain hijacking, or it could have been a renamed file. . . . [T]he extension could have been different than what it actually was." May 20, 2014 Tr. at 62:19-25 (Cravens).

62. Cravens explained that a text file can be changed to look like an image file by double-clicking the name of the file, and "chang[ing] the name and the file extension." May 20, 2014 Tr. at 63:6-8 (Cravens).

63. Cravens did not find, however, any electronic mail transmissions that were labeled to look like other files during his previewing of the CDs. See May 20, 2014 Tr. at 130:17-21 (Cravens, Serna).

64. Although the subscriber account that was used to re-register the Domain was

---

<sup>6</sup>A screen shot is "an image taken by the computer user to record the visible items displayed on the [computer] monitor, television, or another visual output device. Usually, this is a digital image using the operating system or software running on the computer, but it can also be a capture made by a camera or a device intercepting the video output of the display. "Screenshot," Wikipedia.org, <http://en.wikipedia.org/wiki/Screenshot> (last visited Oct. 10, 2014).



created in July, 2009, Cravens did not limit his search to files created after that date, because he believed that the file dates could have been changed or inaccurate. See May 20, 2014 Tr. at 64:4-24 (Cravens, Tuckman).

65. As an example, Cravens explained that, if you change the date on your computer, “it would change all files created or modified after that, the dates would be different, and incorrect.” May 20, 2014 Tr. at 64:19-21 (Cravens).

66. Cravens was not aware, however, whether any of the dates of the files in the electronic media seized from Loera were modified. See May 20, 2014 Tr. at 128:22-129:1 (Cravens, Serna).

67. Aside from the images on those two CDs, Cravens did not find any other child pornography images during the November 20, 2012, search. See May 20, 2014 Tr. at 87:15 (Cravens); id. at 119:21-120:2 (Cravens, Serna).

68. When Nishida began previewing the files on the CDs, he chose not to use a program called “Encase” to limit his search of the CDs to electronic mail transmissions, web pages, or internet history. See Transcript of Hearing at 242:3-25 (Nishida, Serna)(taken May 21, 2014)(“May 21, 2014 Tr.”).

69. Nishida also made a “conscious decision” to not use the FTK Imager software to preview the files, because he thought using Windows Explorer would be faster. May 20, 2014 Tr. at 209:19-22 (Nishida, Serna). See id. at 210:22-211:1 (Nishida, Serna).

70. The FBI also has software that that can determine whether a file’s contents do not match its listed extension -- like a text file with an image extension -- without opening the file itself; Nishida also did not use this program when he previewed the files on the CDs. See May 21, 2014 Tr. at 250:22-251:4 (Nishida, Serna); id. at 251:22-252:7 (Nishida, Serna).

71. Nishida previewed the files using the “details view” -- meaning that he saw a list of files, file names, and last-modified dates of those files, but there were no pictures associated with the files. May 20, 2014 Tr. at 157:13-19 (Nishida, Tuckman).

72. Nishida described his procedure for previewing the files on the CDs as follows:

I would put [CDs] in a laptop. I would open up Windows Explorer, and I would see what was on the CD. I would sample a few files. If it were, say, music files, I would verify that they were what they were labeled. And then I would set it aside. Same if I found the movie “The Wizard of Oz,” I would play it a little bit, see if it was “The Wizard of Oz,” and I would stop it and put it aside.

May 20, 2014 Tr. at 156:19-157:2 (Nishida).

73. Nishida seized only CDs that contained files that appeared to be documents or that he could not immediately identify. See May 20, 2014 Tr. at 158:13-19 (Nishida, Tuckman).

74. Nishida also discovered images of child pornography while previewing the files on the CDs. See May 20, 2014 Tr. at 158:20-22 (Nishida, Tuckman).

75. After finding a child pornography image, Nishida opened two or three other files on that CD to determine if they contained evidence of computer fraud or electronic mail hijacking. See May 20, 2014 Tr. at 161:17-162:18 (Nishida, Tuckman).

76. After finding the first child pornography image, Nishida continued to search for evidence of electronic mail hijacking and computer fraud. See May 20, 2014 Tr. at 165:4-17 (Nishida, Tuckman).

77. Nishida did not limit his search to files that appeared to contain text, because image files could also contain evidence of electronic mail hijacking or computer fraud. See May 20, 2014 Tr. at 163:2-22 (Nishida, Tuckman); id. at 249:11-20 (Nishida, Serna).

78. Nishida also did not limit his search to files created after July, 2009, because the First Warrant did not contain a date restriction, and because he believed that “there could easily

be evidence of the crime that doesn't fit in that data range." May 20, 2014 Tr. at 164:8-11 (Nishida).

79. There are a number of ways in which individuals can change the dates of files on CDs: "[S]ome software will allow you to burn the date, use the dates that were on the hard drives for the files, or use a date that the CD was burned, or you could pick an arbitrary date and just type it in while you're burning . . . the CD." May 20, 2014 Tr. at 219:19-24 (Nishida).

80. Nishida also found a second CD that contained child pornography images. See May 20, 2014 Tr. at 87:15 (Cravens); id. at 119:21-120:2 (Cravens, Serna).

81. Nishida believes that neither he nor Cravens exceeded the scope of the First Warrant during their November 20, 2012, searches of Loera's CDs. See May 21, 2014 Tr. at 253:19-21 (Nishida).

82. In total, the FBI found four CDs containing child pornography images during the November 20, 2012, search -- two from Cravens and two from Nishida. See May 20, 2014 Tr. at 70:20-22 (Cravens, Tuckman).

83. The FBI agents seized nine CDs containing evidence of electronic mail hijacking and computer fraud from Loera's residence. See May 20, 2014 Tr. at 70:23-71:7 (Cravens, Tuckman).

84. In addition to the thirteen CDs, FBI agents also seized several other items from Loera's residence, including computers, external hard drives, an iPhone, and an iPad. See May 20, 2014 Tr. at 39:24-40:8 (Tuckman).

## **2. The November 27, 2012 Searches.**

85. On November 27, 2012, Cravens decided to obtain a search warrant to search the items seized from Loera's residence for child pornography. See May 20, 2014 Tr. at 72:5-12

(Cravens, Tuckman); id. at 140:13-16 (Cravens, Court).

86. Cravens thought that the affidavit in support of the search warrant should include a detailed description of one child pornography image from each of the four CDs on which he and Nishida had found child pornography during their initial preview of the CDs at Loera's residence on November 20, 2012. See May 20, 2014 Tr. at 72:1-4 (Cravens); id. at 72:21-22 (Cravens).

87. Consequently, Cravens obtained the four CDs on which he and Nishida had discovered child pornography from Boady, the Special Agent in charge of Loera's case. See May 20, 2014 Tr. at 71:19-25 (Cravens, Tuckman).

88. Cravens initially tried to preview the images on the first CD using the same FTK Imager software that he had unsuccessfully attempted to use at Loera's residence on November 20, 2012. See May 20, 2014 Tr. at 72:16-17 (Cravens).

89. The FTK software again showed that the CD did not contain any files. See May 20, 2014 Tr. at 72:17-18 (Cravens).

90. Cravens, accordingly, stopped using the FTK software and opened the files on the CDs without it. See May 20, 2014 Tr. at 72:17-22 (Cravens).

91. To find child pornography images that he could accurately describe in the affidavit, Cravens looked at several images -- "more than just a couple" of images, but "[m]ost likely less than a dozen" -- on each of the four CDs seized from Loera's residence. May 20, 2014 Tr. at 143:6-16 (Cravens, Court).

92. That day, Cravens had the four CDs for a total of two-and-a-half hours, during which time he also drafted the Second Affidavit. See May 20, 2014 Tr. at 74:10-21 (Cravens, Tuckman).

93. In the Second Affidavit, Cravens explained that: (i) he had been an FBI agent for eight years; (ii) his experience included investigations of “crimes against children on the Internet”; (iii) computers and electronic media -- including CDs -- are used in the child pornography industry; (iv) child pornography images were found on the four CDs seized from Loera’s residence; and (v) when he used the term “child pornography,” he meant “a visual depiction involving the use of minors engaged in sexually explicit conduct.” See Second Affidavit ¶¶ 2, 6, 8, 23-27, at 1-10.

94. Cravens stated, in the Second Affidavit, that he reviewed the four CDs seized from Loera’s residence on November 27, 2012. See Second Affidavit ¶ 22, at 9.

95. Based on his review of Loera’s CDs on November 27, 2012, Cravens provided a detailed description in the Second Affidavit of three still images and one video of child pornography that he found on Loera’s CDs. See Second Affidavit ¶¶ 23-27, at 8-9.

96. Before submitting his search warrant application to a United States Magistrate Judge, Cravens had John Anderson, the Assistant United States Attorney assigned to Loera’s case, review and approve the application, including the Second Affidavit. See May 20, 2014 Tr. at 75:6-18 (Cravens, Tuckman).

97. On November 29, 2012, the Honorable W. Daniel Schneider, United States Magistrate Judge for the District of New Mexico, approved a search warrant to search the items seized from Loera’s residence for child pornography. See Second Warrant at 1; May 20, 2014 Tr. at 75:22-76:2 (Cravens, Tuckman).

### **3. The Laptop Searches.**

98. On November 28, 2012, Nishida checked out the laptop seized from Loera’s residence from FBI evidence to conduct a search pursuant to the First Warrant. See May 20,

2014 Tr. at 168:1-13 (Nishida, Tuckman).

99. Before a hard drive can be searched for evidence, it must first be “imaged”<sup>7</sup> and “preprocessed.” See May 20, 2014 Tr. at 148:4-5 (Nishida); id. at 168:12-16 (Nishida, Tuckman).

100. The imaging process creates an exact copy of a hard drive. See May 20, 2014 Tr. at 148:4-5 (Nishida).

101. Preprocessing then translates the hard drive data produced by the imaging process from “a group of ones and zeros” into “a form that humans can actually understand.” May 20, 2014 Tr. at 168:12-16 (Nishida, Tuckman).

102. When Nishida conducts a computer search pursuant to a child pornography search warrant, he uses “child pornography hash sets”<sup>8</sup> in the preprocessing procedure. May 20, 2014

---

<sup>7</sup>Imaging creates “an exact . . . copy of the original storage media that exists on the subject computer” -- in this case, the hard drive on Loera’s laptop. “What is Forensic Hard Drive Imaging?” Forensicon Computer Forensic Specialists, [http://www.forensicon.com/wp-content/cache/page\\_enhanced/www.forensicon.com//resources/articles/what-is-forensic-hard-drive-imaging//\\_index\\_ssl.html\\_gzip](http://www.forensicon.com/wp-content/cache/page_enhanced/www.forensicon.com//resources/articles/what-is-forensic-hard-drive-imaging//_index_ssl.html_gzip) (last visited Oct. 13, 2014).

<sup>8</sup>“Hash sets,” also referred to as “hash values,” are created through a process called “hashing,” which,

take[s] a large amount of data, such as a file or all the bits on a hard drive, and use[s] a complex mathematical algorithm to generate a relatively compact numerical identifier (the hash value) unique to that data. Examiners use hash values throughout the forensic process, from acquiring the data, through analysis, and even into legal proceedings. Hash algorithms are used to confirm that when a copy of data is made, the original is unaltered and the copy is identical, bit-for-bit. That is, hashing is employed to confirm that data analysis does not alter the evidence itself. Examiners also use hash values to weed out files that are of no interest in the investigation, such as operating system files, and to identify files of particular interest.

Richard P. Salgado, Fourth Amendment Search and the Power of the Hash, 119 Harv. L. Rev. F. 38 (2005).

Tr. at 169:3-11 (Nishida, Tuckman).

103. Child pornography hash sets filter the hard drive data to determine whether any of the child pornography images on the computer are of a known child pornography victim. See May 20, 2014 at 169:12-170:11 (Nishida, Tuckman).

104. Because Nishida was preprocessing the hard drive only for evidence of electronic mail hijacking and computer fraud pursuant to the First Warrant, however, he did not use the child pornography hash sets on November 28, 2012. See May 20, 2014 Tr. at 169:10-11 (Nishida); id. at 170:12-23 (Nishida, Tuckman).

105. After conducting the initial preprocessing and imaging of the hard drive on Loera's laptop on November 28, 2012, Nishida received the Second Warrant and the Second Affidavit. See May 20, 2014 Tr. at 171:19-25 (Nishida, Tuckman).

106. Nishida did not think there was anything wrong with the Second Warrant. See May 20, 2014 Tr. at 172:1-3 (Nishida, Tuckman).

107. Nishida did not review any of the data that the imaging and preprocessing procedures produced until after he received the Second Warrant. See May 20, 2014 Tr. at 171:9-12 (Nishida, Tuckman).

108. Beginning in December, 2012, Nishida conducted a full examination of the hard drive data from Loera's laptop for the evidence that the First Warrant and the Second Warrant sought. See May 20, 2014 Tr. at 172:4-7 (Nishida, Tuckman); id. at 176:18-185:22 (Nishida,

---

Perhaps the quickest method to find files relevant to your case is through a hash comparison of files against one or more preconfigured hash sets. . . . This process can significantly reduce the amount of data that you must review because you can eliminate irrelevant files through both filtering and hiding of duplicate files.

Brett Shavers & Eric Zimmerman, X-Ways Forensics Practitioner's Guide 109 (Chris Katsaropoulos, et al. eds., 2014).

Tuckman).

109. During his search of the laptop seized from Loera's residence, Nishida found: (i) numerous child pornography images in the "My Documents" folder; (ii) websites under the "Bookmarks" tab with titles such as "Jailbait Cam," "Lot of preteens," and "Lolita Danny"; (iii) a file on the desktop entitled "Allmyfiles.txt" that contained multiple references to child pornography, including -- "11yo Maria Antonio," "10yo Kopia," "14 yo-Lil-And-Girlfriend," and "Spycam 9yr Undress"; and (iii) another file on the desktop entitled "v.txt" that referenced a file named "Vicky 10yo Anal Pumped (33m52s)." May 20, 2014 Tr. at 181:12-185:24 (Nishida, Tuckman). See Jason Loera Dell User Movie CHILD PORNOGRAPHY, submitted to the Court at the May 20, 2014, evidentiary hearing as Government's Hearing Exhibit 11 ("Loera Dell Movie").

110. In total, Nishida found over 730 images and forty movies of child pornography on Loera's laptop. See May 20, 2014 Tr. at 186:22-25 (Nishida, Tuckman).

111. There were so many child pornography images and movies on the laptop that, at some certain point, Nishida stopped counting them. See May 20, 2014 Tr. at 186:25-187:5 (Nishida, Tuckman).

112. If Cravens had not obtained the Second Warrant, Nishida would not have searched the laptop for evidence of child pornography, but he would still have searched it for evidence of electronic mail hijacking and computer fraud pursuant to the First Warrant. See May 20, 2014 Tr. at 187:6-17 (Nishida, Tuckman).

113. While searching for evidence of electronic mail hijacking or computer fraud, Nishida would have clicked on electronic mail transmissions, internet history, internet cache, "Bookmarks," and text files -- including "My Documents," "Allmyfiles.txt" and "v.txt" -- all of



which either contained or referenced child pornography. May 20, 2014 Tr. at 187:18-188:21 (Nishida, Tuckman); Loera Dell Movie.

114. Nishida stated that, had he found child pornography images on the laptop during a search conducted solely pursuant to First Warrant, he would have “alerted the case agent so that [he] could get a search warrant for child pornography.” May 20, 2014 Tr. at 189:8-11 (Nishida).

**4. Nishida’s April, 2013, Searches of Loera’s CDs.**

115. On or about April 4, 2013, Boady asked Nishida to examine the four CDs seized from Loera’s residence for child pornography. See New Mexico Computer Forensics Laboratory Report of Examination at 1 (dated April 19, 2013), submitted to the Court at the May 20, 2014 evidentiary hearing as Government Exhibit 14 (“Apr. 19, 2013, Examination Report”).

116. At some point between April 4, 2013, and April 19, 2013, Nishida attempted to conduct, pursuant to the Second Warrant, a forensic examination for child pornography of the four CDs seized from Loera’s residence. See Apr. 19, 2013, Examination Report at 1.

117. As he had done with the hard drive from Loera’s laptop, Nishida first attempted to image -- or create an exact copy of the data from -- Loera’s CDs. See Apr. 19, 2013, Examination Report at 2; May 20, 2014 Tr. at 215:21-216:11 (Nishida, Serna).

118. Nishida was able to image only two of the four CDs seized from Loera’s residence, however, because two of the CDs “were scratched.” Apr. 19, 2013, Examination Report at 2; May 20, 2014 Tr. at 215:21-216:11 (Nishida, Serna).

119. Consequently, Nishida examined only those two CDs for child pornography. See Apr. 19, 2013, Examination Report at 2.

120. Nishida discovered approximately 330 images and two movies of suspected child pornography on the two CDs that he examined. See Apr. 19, 2013, Examination Report at 2.

## **PROCEDURAL BACKGROUND**

A federal grand jury indicted Loera on two counts of receipt of visual depictions of minors engaged in sexually explicit conduct, allegedly occurring on September 6, 2009, and one count of possession of a visual depiction of a minor engaged in sexually explicit conduct, allegedly occurring on February 20, 2010. See Indictment at 1-2, filed May 29, 2013 (Doc. 2). Early in 2014, a federal grand jury filed a superseding indictment that charged Loera with three counts of possession of material containing any visual depiction of a minor engaged in sexually explicit conduct, each allegedly occurring in November 20, 2012. See Superseding Indictment at 1-2, filed January 9, 2014 (Doc. 25)(“Superseding Indictment”). Count I of the Superseding Indictment concerns the hard drive on Loera’s laptop, and counts 2 and 3 each concern a CD seized from Loera’s residence. See Superseding Indictment at 1-2.

### **1. Loera’s Motion.**

Loera filed the Motion on March 7, 2014. See Motion at 1; Memorandum in Support of Motion to Suppress Evidence and Statements, filed March 7, 2014 (Doc. 36)(“Memorandum”). Loera moves the Court, pursuant to rules 12(b)(3) and 41(f) of the Federal Rules of Criminal Procedure, and pursuant to the Fourth and Fifth Amendments to the Constitution of the United States of America, for an order suppressing the following evidence at trial: (i) all evidence seized from Loera’s effects pursuant to the United States’ illegal search at Loera’s residence on November 20, 2012; (ii) all evidence seized from Loera’s effects pursuant to the United States’ illegal search of Loera’s effects on November 27, 2012; (iii) all evidence seized as a result of the search warrant issued on November 29, 2012; and (iv) all other evidence, tangible or intangible resulting from any illegal searches of Loera’s effects on November 20, 2012, November 27, 2012, and December 7, 2012, and thereafter. See Motion at 1-2.

Loera first argues that the First Warrant lacked particularity, because it failed to specify “‘as nearly as possible the distinguishing characteristics of the goods to be seized.’” Memorandum at 4 (quoting Cassady v. Goering, 567 F.3d 628, 635 (10th Cir. 2009)). Loera next argues that the November 20, 2012, search of the CDs at his residence went beyond the scope of the First Warrant in three ways. See Memorandum at 2-6. First, Loera contends that the First Warrant did not authorize Nishida and Cravens to open images or videos. See Memorandum at 4. Loera says that the First Warrant limited the scope of the November 20, 2012, search to “evidence pertaining to . . . unlawful interception of wire communications and fraud in relation to computers.” Memorandum at 4. In Loera’s view, the First Affidavit “contained no basis for probable cause to believe that evidence of wire fraud or unlawful interception of wire communications would be found in graphic image or video files.” Memorandum at 5 (citing United States v. Sells, 463 F.3d 1148, 1157 (10th Cir. 2006)). Second, Loera asserts that, because the First Affidavit alleged that the wire fraud and interception of wire communications began on July 29, 2011, the First Warrant authorized Cravens and Nishida to only open files created after that date. See Memorandum at 6. Third, Loera contends that the First Warrant did not authorize Cravens and Nishida to continue previewing the CDs after Cravens discovered child pornography. See Memorandum at 8-9 (citing United States v. Carey, 172 F.3d 1268 (10th Cir. 1999)). By doing so, Loera argues, Nishida and Cravens “transformed the search warrant for evidence of . . . wire fraud pertaining to Governor Martinez’s e-mails into a ‘general warrant’ and resulted in a general and illegal search of the four CDs.” Memorandum at 7.

Loera next argues that the November 27, 2012, searches -- Cravens’ search of the four CDs and Nishida’s search of Loera’s laptop -- exceeded the scope of the First Warrant. See

Memorandum at 10-11. Loera argues that “[t]hese . . . searches for child pornography were not within the scope of the November 19 warrant for evidence of wire fraud and unlawful interception of electronic communications.” Memorandum at 11. Finally, Loera asserts that, because the November 20, 2012, and November 27, 2012, searches were unconstitutional, and Cravens relied on those searches to obtain the Second Warrant, the Court should suppress any evidence obtained through the execution of the Second Warrant as fruit of the poisonous tree. See Memorandum at 11.

## **2. The United States’ Response.**

The United States filed a Response to the Motion on April 7, 2014. See United States’ Response to Motion to Suppress Evidence (Doc. 35), filed April 7, 2014 (Doc. 41)(“Response”). In its Response, the United States asks the Court to deny the Motion. See Response at 1. The United States first argues that Loera fails to establish the requisite standing to seek suppression of the child pornography, because he has not asserted a possessory interest in the evidence that he seeks to suppress. See Response at 6-7. The United States next asserts that, to the extent that Loera argues that the First Warrant was not sufficiently particularized, “it is worth noting that the Tenth Circuit has ‘adopted a somewhat forgiving stance’” when faced with particularity challenges to warrants authorizing computer searches. Response at 6 n.4 (quoting United States v. Grimmett, 429 F.3d 1263, 1270 (10th Cir. 2006)). The United States argues that, a warrant authorizing a computer search is sufficiently particular if it is “limited to a search for evidence of a violation of a particular federal statute.” Response at 6 n.4 (citing United States v. Christie, 717 F.3d 1156, 1165 (10th Cir. 2013)).

The United States next contends that the November 20, 2012, search of the CDs at Loera’s residence was within the First Warrant’s scope. See Response at 6-10. The United

States points out that the First Warrant “authorized agents to search and seize, among other things, pictures that could be found on ‘physical objects upon which computer data can be recorded/stored,’ such as the CDs at issue here.” Response at 7 (quoting Attachment B ¶¶ 3, 3a., at 3)). The United States also argues that the First Warrant authorized Nishida and Cravens to open files that appeared to be images and videos, because file names and extensions can be changed to conceal evidence. See Response at 7 n.5. To support this contention, the United States quotes from United States v. Burgess, 576 F.3d 1078 (10th Cir. 2009), in which the United States Court of Appeals for the Tenth Circuit stated:

It is unrealistic to expect a warrant to prospectively restrict the scope of a search by directory, filename, or extension or to attempt to structure search methods -- that process must remain dynamic . . . . [I]llegal activity may not be advertised even in the privacy of one’s personal computer -- it could be well coded or otherwise disguised.

Response at 7 n.5 (quoting United States v. Burgess, 576 F.3d at 1093-94)(internal quotation marks omitted)).

The United States next addresses Loera’s argument that Nishida and Cravens went beyond the scope of the First Warrant by continuing to search the CDs after finding child pornography. See Response at 8-9. The United States contends that Loera’s reliance on United States v. Carey for this argument is “misplaced.” Response at 8. The United States explains that, in United States v. Carey, after discovering child pornography, an officer abandoned his warrant-authorized search for drug-related evidence “to look for more child pornography,” and did not resume his original search for five hours. Response at 9 (quoting United States v. Carey, 172 F.3d at 1273)(internal quotation marks omitted). The United States argues that, unlike the officer in United States v. Carey, Nishida and Cravens did not abandon their warrant-authorized searches after finding evidence of child pornography, but instead continued to search for

evidence of electronic mail hijacking and computer fraud. See Response at 9 (citations omitted). The United States contends that this difference is significant, because the Honorable Bobby R. Baldock, Senior Judge on the Tenth Circuit, stated in his United States v. Carey concurrence that, “‘f the record showed that Detective Lewis had merely continued his [warrant-authorized] search for drug-related evidence, and, in doing so, continued to come across evidence of child pornography, I think a different result would be required.’” Response at 9 (alterations in Response but not source)(quoting United States v. Carey, 172 F.3d at 1277)(Baldock, J., concurring)).

The United States argues that Cravens’ search of Loera’s CDs on November 27, 2012, was permissible. See Response at 10-11. The United States concedes that, “[g]enerally, law enforcement engaged in a lawful search who wish to abandon that search and begin a focused search for child pornography, need to obtain a search warrant before beginning a child pornography search.” See Response at 11 (citing, e.g., United States v. Burgess, 576 F.3d at 1094-95). The United States asserts, however, that Cravens’ “limited review of some files so that he could include a brief description in his affidavit did not rise to the level of an unlawful search outside the scope of the First Warrant.” Response at 11.

The United States argues that, even without Cravens’ description of the images and video that he saw on Loera’s CDs on November 27, 2012, the Second Affidavit included sufficient probable cause to obtain the Second Warrant. See Response at 14. The United States explains that Cravens stated in the Second Affidavit that: (i) he had been an FBI agent for eight years; (ii) his experience included investigations of “crimes against children on the Internet”; (iii) computers and electronic media -- including CDs -- are used in the child pornography industry; (iv) child pornography images were found on the four CDs seized from Loera’s

residence; and (v) when he used the term “child pornography,” he meant “a visual depiction involving the use of minors engaged in sexually explicit conduct.” Response at 12-13 (citations omitted). The United States further asserts that the Tenth Circuit has recognized that the phrase “child pornography” has a generally understood meaning and referring to images of child pornography provides sufficient probable cause to obtain a search warrant. Response at 13 (citing, e.g., United States v. Haymond, 672 F.3d 948, 959 (10th Cir. 2012); United States v. Cervini, 16 F. App’x 865, 868 (10th Cir. 2001)). The United States argues that, accordingly, the information in the Second Affidavit -- even without descriptions of the images or videos on the CDs -- established sufficient probable cause for Judge Schneider to issue the Second Warrant. See Response at 14.

The United States argues that, even if the Court excises Cravens’ descriptions of the three images and one video from the Second Affidavit and finds that the Second Affidavit did not contain sufficient probable cause to obtain the Second Warrant, the Court should find that Nishida relied on the Second Warrant in good faith when he searched Loera’s laptop and CDs pursuant to the Second Warrant. See Response at 14-16. The United States explains that, under the good-faith exception, “evidence seized pursuant to a warrant issued by a neutral and detached magistrate later found invalid may still be admissible if the executing officer acted in objective good faith and with reasonable reliance on the warrant.” Response at 14 (citations omitted)(internal quotation marks omitted). The United States asserts that Nishida searched Loera’s laptop and CDs for child pornography only after Judge Schneider issued the Second Warrant. See Response at 16. In the United States’ view, Nishida relied on Judge Schneider’s determination that probable cause existed to search those items “reasonably and in good faith.” Response at 16. The United States argues that, consequently, the Court should not suppress any

evidence obtained through the execution of the Second Warrant. See Response at 16.

The United States contends that Cravens also acted in good faith in obtaining the Second Warrant. See Response at 15-16. The United States explains that, in the Second Affidavit, Cravens stated that he opened files on Loera's CDs on November 27, 2012, to provide a description of the files in his search warrant affidavit. See Response at 16. The United States points out that Cravens had Mr. Anderson, an Assistant United States Attorney review his application for the Second Warrant, including the Second Affidavit. See Response at 4, 15. The United States argues that the Tenth Circuit has identified asking a lawyer to approve a search warrant application as one factor that indicates an officer acted in good faith in obtaining a warrant. See Response at 16 (citing United States v. Otero, 563 F.3d 1127, 1134-35 (10th Cir. 2009)). The United States contends that Cravens' actions demonstrate that he "was trying to comply with the law," and that his actions are "not enough to justify exclusion." Response at 16.

The United States further argues that none of the exceptions to the good-faith exception apply in this case. See Response at 16. The United States explains that the Supreme Court has recognized four situations in which the good-faith exception does not apply:

- (1) the issuing judge was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth;
- (2) the issuing judge wholly abandoned his judicial role and failed to perform his neutral and detached role;
- (3) the affidavit issued to support the warrant is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and
- (4) the warrant is so facially deficient that the executing officers cannot reasonably presume it to be valid.

Response at 15 (citations omitted)(internal quotation marks omitted). The United States argues



that Judge Schneider was not misled by any falsehoods, and that he remained neutral and detached. See Response at 15. The United States further contends that the Second Affidavit “overwhelmingly” established probable cause and that there was nothing on the face of the Second Warrant which would lead Nishida to presume it was invalid. Response at 15.

The United States asserts that, even if Cravens had not obtained the Second Warrant, Nishida would have inevitably discovered child pornography while searching the items seized from Loera’s residence pursuant to the First Warrant. See Response at 17. The United States contends that, “evidence obtained in violation of the Fourth Amendment should not be suppressed if agents inevitably would have discovered that evidence through lawful means.” Response at 17 (citing United States v. Christy, 739 F.3d 534, 540 (10th Cir. 2014)). The United States argues that the inevitable discovery inquiry turns on the likelihood “that a warrant would have been issued and that the evidence would have been found pursuant to the warrant.” Response at 17 (quoting United States v. Christy, 739 F.3d at 541)(internal quotation marks omitted).

The United States contends that Loera “had so much readily accessible child pornography on his electronic media that not only would agents have inevitably discovered the contraband while searching under the authority of the First Warrant, they would have done so . . . in a matter of minutes.” Response at 17. The United States explained that, when Nishida searched Loera’s laptop, he quickly found several child pornography sites under the “Bookmarks” tab, a text file on the desktop that contained child pornography terms, and images of child pornography on the laptop itself. Response at 17. Once Nishida found that evidence, the United States contends, he would have obtained a search warrant authorizing a search for child pornography, because “that is exactly what [Cravens and Nishida] did.” Response at 18.

The United States also argues that the four factors from United States v. Souza, 223 F.3d 1197 (10th Cir. 2000), weigh in favor of finding inevitable discovery. See Response at 18. The United States explains that the United States v. Souza factors are:

- 1) the extent to which the warrant process has been completed at the time those seeking the warrant learn of the search;
- 2) the strength of the showing of probable cause at the time the search occurred;
- 3) whether a warrant ultimately was obtained, albeit after the illegal entry; and
- 4) evidence that the law enforcement agents “jumped the gun” because they lacked confidence in their showing of probable cause and wanted to force the issue by creating a fait accompli.

Response at 18 (quoting United States v. Christy, 739 F.3d at 541). Addressing the first factor, the United States argues that the First Warrant and the Second Warrant were obtained before Nishida began searching for child pornography. See Response at 18. Turning to the second factor, the United States contends that the strength of the probable cause showing was “undeniably high” when Nishida searched Loera’s CDs and laptop, because Cravens and Nishida had personally viewed child pornography on the CDs on November 20, 2012. See Response at 18. Regarding the third factor, the United States says that Cravens obtained the Second Warrant and, had there been no Second Warrant, “there is no question that the FBI would have obtained a warrant authorizing a search for child pornography evidence once . . . Nishida found such evidence” during his search under the First Warrant. Response at 19. As to the fourth factor, the United States contends that Nishida and Cravens did not “jump the gun,” but instead had “complete confidence that probable cause existed to support the issuance of a search warrant,” because Nishida waited until he obtained the Second Warrant to conduct the search. Response at 19. The United States concludes its inevitable discovery argument by stating that, “if the Court

finds the Second Warrant to have been invalid, the evidence obtained from the search authorized by the warrant should not be suppressed as it inevitably would have been lawfully discovered.” Response at 19.

### **3. Loera’s Reply.**

Loera filed his Reply to the Response on April 12, 2014. See Defendant’s Reply to United States’ Response to Motion to Suppress Evidence, filed on April 12, 2014 (Doc. 45)(“Reply”). Loera addresses the United States’ standing argument by admitting that the CDs and laptop on which the agents discovered child pornography were in Loera’s control and possession when the agents seized them. See Reply at 1. Loera then reiterates the arguments that he made in his Motion and Memorandum. See Reply at 1-5. Moreover, Loera argues that Attachment B mentioned photographs, not as evidence of wire fraud or unlawful interception of electronic communications, but as ““evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted.”” Reply at 3 (quoting Attachment B ¶ 3.a., at 3).

Loera next turns to the United States’ argument that the Second Warrant would be valid even without Cravens’ description of the three images and one movie that he found on Loera’s CDs. See Reply at 5-6. Loera contends that the resulting search warrant affidavit would read, “four writable CDs . . . appeared to contain images of child pornography.” Reply at 5. In Loera’s view, “child pornography” is a “mere conclusory statement[]” that “cannot support probable cause.” Reply at 6. Loera contends that, accordingly, without the detailed description of the images and video that Cravens obtained from his November 27, 2012, search, the Second Affidavit would not establish probable cause. See Reply at 6.

Loera asserts that the good-faith exception does not apply in this case. See Reply at 6-8.

Loera argues that the First Affidavit was “so lacking in probable cause” to search for child pornography, image or video files, or any file with the date last modified before July 29, 2011, that the FBI agents’ reliance on it was unreasonable. Reply at 7. Loera then addresses the United States’ argument that Cravens’ November 27, 2012, search was permissible:

[T]he government seeks to justify the November 27 searches because Cravens “wanted to provide the Magistrate Judge who issued the Second Warrant with a description of a few of those images” while in the next breath arguing Cravens did not have to actually conduct the November 27 searches because uttering the words “child pornography” was enough for probable cause.

Reply at 7 (quoting Response at 10, 13). In Loera’s view, this “duplicity hardly exudes good faith.” Reply at 7. Loera further states that “the government’s second warrant on November 29 to search for child pornography after it had conducted two warrantless searches . . . also shows a lack of good faith.” Reply at 7. Loera concludes his argument on the applicability of the good-faith exception by asserting:

Despite the existence of Carey, which stated in 1999 that a warrant should be acquired after the first image was seen, the government here proceeded to conduct more searching for child pornography on November 20 and on November 27 before finally seeking a search warrant on November 29 for child pornography. Good faith did not exist.

Reply at 7-8.

Loera challenges the United States’ assertion that it would have inevitably discovered evidence of child pornography while searching for evidence pursuant to the First Warrant. See Reply at 8-9. Loera asserts that “there are a couple of problems with [this] argument.” Reply at 8. First, Loera states that a second search for child pornography based on a warrant seeking evidence of wire fraud and unlawful interception of electronic communications would not lawfully uncover child pornography, because that search would be subject to the same outside the scope analysis as the original November 20, 2012, search. See Reply at 8-9. Second, Loera

argues that “storing websites and ‘child pornography terms’ is distinctly different from having images of child pornography as it pertains to probable cause, and the details of this searching will have to be ferreted out during testimony.” Reply at 9. Finally, Loera contends, without further explanation, that Nishida and Cravens “did not ‘exactly’ proceed to get a warrant to search for child pornography on November 20 or November 27 before seeking the second warrant on November 29.” Reply at 9. In Loera’s view, accordingly, the United States’ conduct “does not infer inevitable discovery.” Reply at 9.

Loera next argues that the four United States v. Souza factors do not weigh in favor of applying the inevitable discovery exception in this case. See Reply at 9 (citing United States v. Souza, 223 F.3d at 1204). Regarding the first factor, Loera contends that “[t]he first warrant was for wire fraud and unlawful interception of electronic communications and the second warrant is invalidated to consider inevitable discovery.” Reply at 9. Addressing the second factor, Loera argues that, “if the evidence of child pornography gained on November 20 and November 27 was unconstitutionally acquired, then there is no evidence of probable cause for child pornography.” Reply at 9. As to the third factor, Loera contends that, “because of the government’s conduct that resulted in consideration of inevitable discovery, there is great question whether a warrant would have been obtained before searching for child pornography.” Reply at 9-10. Regarding the fourth factor, Loera argues that Cravens and Nishida “jumped the gun” on November 20 when they conducted searches that the First Warrant did not authorize. Reply at 10. Loera asserts that Cravens similarly “jumped the gun” on November 27, 2012. Reply at 10. Loera concludes his inevitable discovery argument by stating that, “[b]ecause the second warrant was invalid, the evidence obtained from the searched [sic] authorized by the warrant should be suppressed as it would not inevitably have been lawfully discovered.” Reply at 10.

**4. The May 20 & 21, 2014, Evidentiary Hearing.**

The Court held an evidentiary hearing on May 20, 2014, and May 21, 2014. See May 20, 2014 Tr. at 1-227; May 21, 2014 Tr. at 227-277. In its opening statement, the United States largely reiterated the arguments from its Response. See May 20, 2014 Tr. at 34:21-47:11 (Tuckman, Court). The United States called Cravens and Nishida to testify at the evidentiary hearing. Cravens explained his role in the execution of the First Warrant -- specifically that he was responsible for previewing the CDs at Loera's residence to determine if they contained evidence of electronic mail hijacking or computer fraud. See May 20, 2014 Tr. at 57:23-58:6 (Cravens, Tuckman). Cravens testified that, while previewing the files on the CDs, he discovered a child pornography image on two CDs. See May 20, 2014 Tr. at 60:5-7; id. at 67:18-68:4 (Cravens, Tuckman). Cravens stated that, after finding child pornography on a CD, he ejected the CD from his computer and set it aside to be seized. See May 20, 2014 Tr. at 61:12-13 (Cravens). Cravens stated that, after finding child pornography, he continued to search for evidence of electronic mail hijacking and computer fraud. See May 20, 2014 Tr. at 65:10-17 (Cravens, Tuckman); id. at 116:3-12 (Cravens, Serna).

Cravens explained that, on November 27, 2012, he decided to obtain a search warrant to search the items seized from Loera's residence for child pornography. See May 20, 2014 Tr. at 72:5-12 (Cravens, Tuckman); id. at 140:13-16 (Cravens, Court). Cravens testified that he obtained Loera's CDs from Boady to provide a description of one child pornography image from each of CDs in his search warrant affidavit. See May 20, 2014 Tr. at 71:19-25 (Cravens, Tuckman); id. at 72:1-4 (Cravens); id. at 72:21-22 (Cravens). Cravens stated that, to find child pornography images which he could accurately describe in the affidavit, he looked at several images on each of the four CDs seized from Loera's residence. See May 20, 2014 Tr. at

143:6-16 (Cravens, Court). Cravens testified that he had an Assistant United States Attorney review and approve his application package -- including the Second Affidavit -- before submitting it to Judge Schneider. See May 20, 2014 Tr. at 75:6-18 (Cravens, Tuckman). Cravens stated that he submitted his search warrant application to Judge Schneider, who then issued the Second Warrant. See May 20, 2014 Tr. at 75:22-76:2 (Cravens, Tuckman).

The United States called Nishida to testify at the evidentiary hearing. See May 20, 2014 at 144:1-9 (Tuckman, Court). Nishida explained that, during the execution of the First Warrant on November 27, 2012, he was responsible for previewing the files on the CDs found at Loera's residence to determine if they contained evidence of electronic mail hijacking and computer fraud. See May 20, 2014 Tr. at 155:8-24 (Nishida, Tuckman). Nishida testified that he discovered images of child pornography on two CDs found at Loera's residence. See May 20, 2014 Tr. at 87:15 (Cravens); id. at 119:21-120:2 (Cravens, Serna); id. at 158:20-22 (Nishida, Tuckman). Nishida stated that, after finding a child pornography image on a CD, he opened two or three other files on that CD to determine if they contained evidence of computer fraud or electronic mail hijacking. See May 20, 2014 Tr. at 161:17-162:18 (Nishida, Tuckman). Nishida testified that he continued to search for evidence of electronic mail hijacking and computer fraud after finding child pornography images. See May 20, 2014 Tr. at 165:4-17 (Nishida, Tuckman).

Nishida explained that, on November 28, 2012, he checked Loera's laptop out of FBI evidence to search it pursuant to the First Warrant. See May 20, 2014 Tr. at 168:1-13 (Nishida, Tuckman). Nishida testified that, before conducting a full search, he first had to "preprocess" and "image" the laptop's hard drive. May 20, 2014 Tr. at 168:1-13 (Nishida, Tuckman). Nishida testified that he received the Second Warrant and the Second Affidavit after conducting the initial preprocessing and imaging of Loera's laptop. See May 20, 2014 Tr. at 171:19-25

(Nishida, Tuckman); id. at 172:1-3 (Nishida, Tuckman). Nishida stated that, beginning in December of 2012, he conducted a full examination of Loera's laptop for the evidence that the First Warrant and the Second Warrant sought. See May 20, 2014 Tr. at 172:4-7 (Nishida, Tuckman); id. at 176:18-185:22 (Nishida, Tuckman).

Nishida testified that, during his search of Loera's laptop, he found child pornography images in the "My Documents" folder, child pornography websites under the "Bookmarks" tab, and at least two files on the desktop that referenced child pornography. May 20, 2014 Tr. at 181:12-185:24 (Nishida, Tuckman). Nishida stated that, if Cravens had not obtained the Second Warrant, he would not have searched the laptop for evidence of child pornography, but he would still have searched it for evidence of electronic mail hijacking and computer fraud pursuant to the First Warrant. See May 20, 2014 Tr. at 187:6-17 (Nishida, Tuckman). Nishida testified that, while searching for evidence of electronic mail hijacking or computer fraud, he would have clicked on electronic mail transmissions, internet history, internet cache, the "Bookmarks" tab, and text files -- all of which either contained or referenced child pornography. May 20, 2014 Tr. at 187:18-188:21 (Nishida, Tuckman). Nishida stated that, had he found child pornography images on the laptop during a search conducted solely pursuant to First Warrant, he would have "alerted the case agent so that [he] could get a search warrant for child pornography." May 20, 2014 Tr. at 189:8-11 (Nishida).

##### **5. Loera's Supplement to the Reply.**

Loera filed a supplement to his Reply on August 18, 2014. See Defendant's Supplement to Reply to United States' Response to Motion to Suppress Evidence, filed August 18, 2014 (Doc. 55)("Supplement to Reply"). Loera first addresses the United States' inevitable discovery argument. See Supplement to Reply at 2. Loera asserts that "[t]he Tenth Circuit has emphasized



the danger of admitting unlawfully obtained evidence on the strength of some judge's speculation that it would have been discovered legally anyway." Supplement to Reply at 2 (quoting United States v. Owens, 782 F.2d 146, 152-53 (10th Cir. 1986)(internal quotation marks omitted)). Loera then states:

"If the prosecution can establish by a preponderance of the evidence that the information ultimately or inevitably would have been discovered by lawful means . . . then the deterrence rationale has so little basis that the evidence should be received." . . . This Court should not be convinced a preponderance of the evidence shows the police would have sought a third search warrant if the second warrant was invalid.

Supplement to Reply at 2-3 (quoting Nix v. Williams, 467 U.S. 431, 444 (1984)).

Loera next argues that Nishida and Cravens did not have probable cause to open any files on Loera's CDs dated before July 29, 2011. See Supplement to Reply at 3-7. Loera explained that Cravens and Nishida testified that "dates did not matter regarding what could be examined on Mr. Loera's storage media and computer," and, if they paid attention to dates, they could miss evidence. Supplement to Reply at 4 (citations omitted). Loera argues that there are three problems with the agents' approach. See Supplement to Reply at 4.

First, Loera contends that disregarding the file dates turned the First Warrant into a "general exploratory warrant" that the Tenth Circuit and the Supreme Court have found unconstitutional. Supplement to Reply at 4. Second, Loera states that, "dates actually do matter." Supplement to Reply at 4. Loera argues that, contrary to the United States' assertion that the First Warrant did not put any restriction on time or dates, the First Affidavit only sought emails sent "during the period of time the Domain is believed to have been compromised by [Loera and Estrada]" -- which began on July 29, 2011. Supplement to Reply at 5 (emphasis in Supplement to Reply but not source)(quoting First Affidavit at 8). Loera asserts that, "[c]onsequently, regardless of what method, manner or mode used by government agents to view

or search Mr. Loera's storage media or computer, the November 19 search warrant could not and did not authorize opening any files dated in 2009, or otherwise from prior to July 29, 2011." Supplement to Reply at 5.

Third, Loera challenges the United States' contention that Cravens and Nishida could disregard the file dates, because they could have been changed. See Supplement to Reply at 6. Loera argues that there was "not a single indication" in the First Warrant and its Attachments that the dates of the files on Loera's computer or CDs were changed. Supplement to Reply at 6. Loera asserts that this is "particularly important," because the First Affidavit focused on the importance of dates at multiple points. Supplement to Reply at 6. For example, Loera states that the First Affidavit sought "'forensic electronic evidence that establishes how computers were used, . . . and when.'" Supplement to Reply at 6 (emphasis in Supplement to Reply but not source)(quoting First Affidavit at 13-14). Loera points out that the First Affidavit states that, "'(and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time'. . . and . . . twice stated it was important to know 'when' the computer was used.'" Supplement to Reply at 6 (citations omitted)(emphasis in Reply but not First Affidavit).

Loera states that Cravens "admitted he was not aware of any evidence that dates on files had been changed." Supplement to Reply at 6 (citations omitted). Loera further points out that, although Nishida testified that file dates on CDs could be changed and that he knew of software that would do so, he did not know how common it is. See Supplement to Reply at 6 (citations omitted). Turning briefly to his particularity argument, Loera asserts that "[t]he agents' testimony that [the First Warrant] did not contain a restriction pertaining to time or dates of the files . . . supports invalidation of the warrant" for lack of particularity, because it failed to specify

“as nearly as possible the distinguishing characteristics of the goods to be seized.” Supplement to Reply at 6-7 (quoting Cassady v. Goering, 567 F.3d at 635).

Loera next argues that the First Affidavit did not provide probable cause to believe that image or video files on Loera’s CDs or laptop would contain the evidence that the First Warrant sought. See Supplement to Reply at 7. Loera points out that the First Affidavit did not allege that Estrada intercepted images or videos through the electronic mail accounts at the Domain. See Supplement to Reply at 7. Loera contends that, accordingly, the First Warrant did not authorize Cravens and Nishida to open image or video files on Loera’s laptop or CDs -- even if they were dated on or after July 29, 2011. See Supplement to Reply at 7.

Loera next addresses the United States’ argument that Nishida would have inevitably discovered child pornography when he searched Loera’s laptop pursuant to the First Warrant. See Supplement to Reply at 12. Loera first argues that, without the Second Warrant, Nishida would have discovered child pornography only if he had exceeded the scope of the First Warrant by clicking on images and video files. See Supplement to Reply at 13-14 (citing Nix v. Williams; Walter v. United States, 447 U.S. 649, 654 (1980)). Loera next contends that there is “no evidence” that Nishida or anyone else would have sought another search warrant if Nishida discovered child pornography on Loera’s laptop. Supplement to Reply at 13. Loera explains:

Nishida was not an affiant in seeking either of the two existing search warrants in this case. After allegedly finding child pornography on two CDs on November 20, Nishida personally did not author or seek a search warrant to search the Dell laptop. Only after Cravens had conducted his unlawful warrantless search of the CDs for child pornography on November 27, did Cravens, not Nishida seek the second search warrant, which included the Dell laptop.

Supplement to Reply at 13. Loera also asserts that, had Nishida discovered child pornography on Loera’s laptop while executing the First Warrant, Boady also would not have obtained a

search warrant for child pornography, because Boady did not do so after Cravens told Boady that he found child pornography on Loera's CDs on November 20, 2012. See Supplement to Reply at 13. Loera concludes his inevitable discovery argument by contending that "[t]he historical facts fail to show with sufficient probability that Nishida would have sought a search warrant after finding child pornography on the laptop." Supplement to Reply at 13.

**6. The August, 19, 2014, Hearing.**

The Court held a hearing on August 19, 2014, to hear the parties' closing arguments on the Motion. See Transcript of Hearing (taken August 19, 2014)("Aug. 19, 2014 Tr."). Loera argued that, in the computer context, it is especially important that the search warrant is narrowly drafted, because of all of the lawful, private information that a computer may contain. See Aug. 19, 2014 Tr. at 285:17-21 (Serna). Loera reiterated that the First Warrant was not sufficiently particular, because it failed to "specify as nearly as possible the distinguishing characteristics of the goods to be seized." Aug. 19, 2014 Tr. at 298:24-299:4 (Serna)(citing Cassady v. Goering).

Loera next asserted that Cravens and Nishida exceeded the First Warrant's scope when they searched Loera's CDs on November 20, 2012. See Aug. 19, 2014 Tr. at 285:11-22 (Serna). In Loera's view, because Nishida and Cravens had access to software that would allow them to restrict their searches to text files and files modified after July 29, 2011, yet failed to use them, their searches were unconstitutional. See Aug. 19, 2014 Tr. at 287:23-288:4 (Serna); id. at 290:12-292:14 (Serna). Loera also highlighted that Nishida admitted it would not have been impractical to seize all of the media items from Loera's house, take them to the FBI lab, and search them using the search-limiting software. See Aug. 19, 2014 Tr. at 292:15-25 (Serna).

The Court noted that it was struck by the First Warrant's breadth and suggested that Loera would have to argue that the warrant lacked particularity, rather than that the agents'

searches exceeded the scope of the First Warrant. See Aug. 18, 2014 Tr. at 288:5-11 (Court); id. at 288:1-6 (Court). Upon questioning by the Court, Loera would not concede that the First Warrant was broad enough to cover the files that Nishida and Cravens opened. See Aug. 19, 2014 Tr. at 289:10-18 (Serna, Court).

Loera reiterated his argument from the Supplement to the Reply that the First Warrant did not authorize Nishida and Cravens to open files that were last modified before July 29, 2011. See Aug. 19, 2014 Tr. at 294:18-295:22 (Serna). The Court inquired whether there was any force to the United States' argument that it did not have to impose a date restriction on its search, because file dates can be inaccurate. See Aug. 19, 2014 Tr. at 296:2-9 (Court); id. at 296:15-21 (Court). Loera rejected that argument, explaining that even the United States believed that the file dates on Loera's CDs and laptop were reliable. See Aug. 19, 2014 Tr. at 297:2-5 (Serna). Loera pointed to the numerous sections of the First Affidavit and Attachment B that discuss the importance of file creation and last accessed dates, and sought "all financial records from June 2011 to the present." Aug. 19, 2014 Tr. at 297:6-17 (Serna). Loera explained that he was not arguing that the file dates on Loera's laptop and CDs were "off somewhat." Aug. 19, 2014 Tr. at 297:18-19 (Serna). Loera pointed out that there is a two-to-three year difference between the alleged electronic mail hijacking and computer fraud that the First Warrant focused on -- which began in 2011 -- and the files that Cravens and Nishida opened -- which contained last-modified dates from 2008 and 2009. See Aug. 19, 2014 Tr. at 297:19-298:2 (Serna).

The Court inquired whether Loera had any case law, which says that, if law enforcement has tools at a different location that may narrow the search, the Constitution requires that they seize everything and conduct the search with those tools at the other location. See Aug. 19, 2014 at 299:19-300:14 (Court). Loera responded that he was not aware of any such case law, but, in

his view, using those tools would have “ensur[ed] that law enforcement [was] staying within the bounds of the Constitution.” Aug. 19, 2014 Tr. at 300:15-301:10 (Serna). Loera then reiterated his arguments that Cravens and Nishida exceeded the scope of the First Warrant when they opened image and video files, and when they continued opening files on the CDs after discovering child pornography. See Aug. 19, 2014 Tr. at 305:5-308:3 (Serna). Loera also argued that, after finding child pornography, Cravens and Nishida abandoned their search for electronic mail hijacking and computer fraud, and began searching for child pornography -- and, in doing so, ran afoul of the Tenth Circuit’s decision in United States v. Carey. See Aug. 19, 2014 Tr. at 326:2-14 (Serna).

The United States conceded that Loera had sufficient standing to move to suppress the child pornography evidence. See Aug. 19, 2014 Tr. at 314:21-315:3 (Tuckman). The United States then argued that the law did not require Cravens and Nishida to seize everything from Loera’s residence and analyze it at the FBI laboratory with search-limiting software. See Aug. 19, 2014 Tr. at 315:12-318:13 (Tuckman). The United States explained that the Tenth Circuit “has been clear that computer searches are fluid, they’re dynamic. You don’t set out a methodology ahead of time saying what you have to do; that you can only look for this type of file or this type of extension.” Aug. 19, 2014 Tr. at 315:13-18 (Tuckman). As an example, the United States cited United States v. Burgess, in which the Tenth Circuit explained that, if United States agents are executing a search warrant and come upon a folder that says “2002 tax records,” they can look through that folder to make sure it actually is 2002 tax records, and not anything else that someone engaged in criminal activity might be trying to hide. Aug. 19, 2014 Tr. at 315:22-316:7 (Tuckman). The United States contended that it would be unreasonable to force Cravens and Nishida to limit their search to specific file names or types, because there was

no way of knowing how Loera concealed evidence of the electronic mail hijacking and computer fraud. See Aug. 19, 2014 Tr. at 317:2-13 (Tuckman). The United States then reiterated its argument that Cravens and Nishida were not required to stop searching the CDs once they found child pornography. See Aug. 19, 2014 Tr. at 319:13-16 (Tuckman).

In response, Loera explained that his “argument is not that there is some constitutional requirement that . . . the law enforcement take everything back to the lab,” but instead that it would have been practical and constitutional for them to do so. Aug. 19, 2014 Tr. at 323:22-25 (Serna). The Court stated that it was inclined to find that the agents’ preview of the files on the CDs on November 20, 2012, was within the First Warrant’s scope. See Aug. 19, 2014 Tr. at 324:21-325:1 (Court). The Court explained that, as long as Cravens and Nishida continued to look for evidence of electronic mail hijacking and computer fraud after finding the child pornography -- as the Court believed they did -- they were not required to use the least restrictive means to conduct their searches. See Aug. 19, 2014 Tr. at 325:2-10 (Court).

Loera then repeated the argument from his Motion and Reply that Cravens’ November 27, 2012, search of Loera’s CDs was unconstitutional. See Aug. 19, 2014 Tr. at 326:21-327:18 (Serna). The Court asked why the Second Affidavit -- without the descriptions that Cravens obtained from his November 27, 2012, search -- did not provide sufficient probable cause for a search warrant. See Aug. 19, 2014 Tr. at 327:19-328:7 (Court); id. at 328:7-17 (Court). Loera responded that, without Cravens’ descriptions, the Second Affidavit would state only that Cravens found “child pornography” -- which is a “mere conclusory statement” that would not provide probable cause. Aug. 19, 2014 Tr. at 328:18-329:13 (Serna); id. at 335:15-336:2 (Serna)(citing United States v. Roach, 582 F.3d 1192, 1203 (10th Cir. 2009)). In Loera’s view, the warrant affidavit would have to include a description of the child pornography, or some

factual basis why Cravens concluded it was child pornography, to establish probable cause. See Aug. 19, 2014 Tr. at 329:14-330 (Court, Serna).

In response, the United States reiterated its arguments from the Response and asserted that it could not find any cases indicating whether Cravens' actions on November 27, 2012, were permissible. See Aug. 19, 2014 Tr. at 330:24-331:2 (Tuckman); id. at 331:24-333:5 (Tuckman). The United States concluded that "it might have been a better tack" for Cravens to have waited to review the CDs until after he obtained the Second Warrant. Aug. 19, 2014 Tr. at 331:2-3 (Tuckman).

The United States argued that the Second Affidavit -- with Cravens' descriptions of the child pornography excised -- established probable cause. See Aug. 19, 2014 Tr. at 333:16-334:25 (Tuckman, Court). The United States argued that the Tenth Circuit has recognized that child pornography is "one of those terms people know what it means when they say it." Aug. 19, 2014 Tr. at 333:19-20 (Tuckman). The United States pointed out that the Second Affidavit not only contained the phrase "child pornography," it also provided a definition of that phrase -- "children engaging in sexually explicit conduct" -- and described Cravens' experience in child pornography matters. Aug. 19, 2014 Tr. at 333:20-24 (Tuckman). The United States explained that the situation is similar to one in which a Drug Enforcement Agency agent is trying to obtain a warrant for a house, and explains in the warrant affidavit that he has been an agent for twelve years, has extensive experience with drugs, and smelled the odor of marijuana coming from the home. See Aug. 19, 2014 Tr. at 336:4-17 (Tuckman). The United States contended that -- even with Cravens' description of the child pornography excised -- there was sufficient information in the Second Affidavit to obtain a search warrant. See Aug. 19, 2014 Tr. at 334:24-25 (Tuckman).



Loera responded that, unlike child pornography, the smell of marijuana does not have a statutory definition. See Aug. 19, 2014 at 336:25-337:2. Loera stated that “the fact that Agent Cravens felt it necessary to put a description in there, and Agent Boady, the case agent, his supervisor, apparently felt it necessary to put some kind of description in there . . . is important.” Aug. 19, 2014 at 337:3-8 (Serna). The Court stated that it tended to agree with Loera that Cravens’ November 27, 2012, search was unconstitutional, and that it should, accordingly, excise any description obtained from that search from the Second Affidavit. See Aug. 19, 2014 Tr. at 337:10-23 (Court). The Court noted, however, that it was inclined to agree with the United States that the remaining information in the Second Affidavit established probable cause. See Aug. 19, 2014 at 337:24-338:6 (Court).

Loera next argued that the good-faith exception should not apply. See Aug. 19, 2014 at 340:10-346:5 (Serna, Court). Loera contended that Cravens did not act in good faith in obtaining the Second Warrant, because neither he nor Boady consulted an Assistant United States Attorney before searching the CDs for images of child pornography on November 27, 2012. See Aug. 19, 2014 at 340:10-24 (Serna). Loera argued that United States v. Herring, 555 U.S. 135 (2009), is not applicable to this case, because Cravens both conducted the unlawful search on November 27, 2012, and authored the Second Affidavit. See Aug. 19, 2012 at 341:5-10 (Tuckman).

Loera then asserted that part of the good-faith analysis is looking at whether excluding evidence in a particular case furthers the policies underlying the exclusionary rule. See Aug. 19, 2014 at 345:10-15 (Serna). Loera argued that,

in this case, we know what Cravens did. It’s our position that he shouldn’t have done that. And the policies are furthered by the application of the Exclusionary Rule, because this is something that he knew, or should have known that he shouldn’t have done. This isn’t a situation where a cop is simply executing a warrant that he didn’t play any hand in, doesn’t know anything about, kind of like the Herring case. This isn’t that situation. This is where the bad actor is the same

guy that's drafted the warrant and, you know, would have executed the warrant.

Aug. 19, 2014 Tr. at 345:16-346:1 (Serna).

In response, the United States argued that the Tenth Circuit has identified consulting a lawyer about the search warrant application as a factor indicating that an officer acted in good faith in obtaining a warrant -- which is exactly what Cravens did. See Aug. 19, 2014 Tr. at 346:17-21 (Tuckman). The United States explained that Cravens stated in the Second Affidavit that he reviewed the CDs to provide a description in the affidavit. See Aug. 19, 2014 Tr. at 347:3-6 (Tuckman). In the United States' view, rather than "try[ing] to hide anything," Cravens "laid out exactly what he had done." Aug. 19, 2014 Tr. at 347:18-19 (Tuckman). The United States explained that Nishida executed the Second Warrant. See Aug. 19, 2014 Tr. at 348:7-9 (Tuckman). The United States argued that, when Nishida did so, he knew that an Assistant United States Attorney had reviewed it, and that Judge Schneider had approved it. See Aug. 19, 2014 Tr. at 348:7-14 (Tuckman). The United States asserted that Herring v. United States applies, and that the good-faith inquiry, accordingly, turns on whether Nishida's unlawful conduct in executing the Second Warrant was "a systemic error, or . . . such a blatant disregard of constitutional law . . . that 'any marginal deterrence does not pay its way.'" Aug. 19, 2014 Tr. at 348:18-22 (Tuckman)(quoting Herring v. United States, 555 U.S. at 147-148).

The United States argued that Cravens "was trying to do everything right." Aug. 19, 2014 Tr. at 348:25-349:1 (Tuckman). The United States explained that, after discovering child pornography, Cravens set aside Loera's CDs to obtain a second warrant, drafted a search warrant affidavit, had it reviewed by an Assistant United States Attorney, presented it to Judge Schneider, and only then did Nishida conduct his search. See Aug. 19, 2014 Tr. at 349:1-7 (Tuckman). In the United States' view, these actions "exude" good faith. Aug. 19, 2014 Tr. at

349:7 (Tuckman). The United States concluded its argument on the good-faith exception by explaining that the Court does not have to reach the good-faith issue if it excises Cravens' description of the child pornography and finds that the Second Warrant was nevertheless valid. See Aug. 19, 2014 Tr. at 351:9-16 (Tuckman).

Loera responds that the good-faith exception does not apply to Nishida's execution of the Second Warrant, because Nishida knew that Cravens was involved in the unlawful searches that occurred on November 20, 2012, and November 27, 2012. See Aug. 19, 2014 Tr. at 356:5-7 (Serna). In Loera's view, Nishida's involvement in the investigation predating the Second Warrant "puts him more on notice that there is . . . an issue here; that he's not acting completely in good faith." Aug. 19, 2014 Tr. at 356:23-25 (Serna). The Court stated that it is always struck by how broadly the Tenth Circuit applies the good-faith exception, and that it believes the good-faith inquiry focuses on the executing officer, and not on the officer who drafted the search warrant affidavit. See Aug. 19, 2014 Tr. at 357:4-19 (Court). The Court said that, if the inquiry focuses on the executing officer, it is inclined to find that Nishida acted in good faith. See Aug. 19, 2014 Tr. at 357:12-358:4 (Court).

Turning to the inevitable discovery issue, Loera repeated his arguments from the Supplement to the Reply -- namely: (i) that Nishida would not have discovered child pornography while executing the First Warrant unless he went beyond the scope of the First Warrant by clicking on image and video files; and (ii) had Nishida discovered child pornography on Loera's laptop while executing the First Warrant, neither he nor Boady would have obtained a second search warrant for child pornography. See Aug. 19, 2014 Tr. at 360:17-362:5 (Serna); id. at 364:17-366:14 (Serna). The United States responded that Nishida inevitably would have discovered child pornography on Loera's laptop, because -- as the Loera Dell Movie indicated --

Nishida discovered child pornography and references to child pornography in many of the places that he would have searched when he executed the First Warrant. See Aug. 19, 2014 Tr. at 363:6-21 (Tuckman); id. at 364:7-13 (Tuckman). The United States then reiterated the argument from its Response that the four factors from United States v. Souza weigh in favor of finding inevitable discovery. See Aug. 19, 2014 Tr. at 363:22-364:6 (Tuckman); id. at 370:20-25 (Tuckman). Upon questioning by the Court, the United States conceded that the inevitable discovery and good-faith exceptions do not save any problems with the November 20, 2012, searches, but instead apply only to the searches that Nishida conducted pursuant to the Second Warrant. See Aug. 19, 2014 Tr. at 373:22-374:5 (Tuckman, Court).

The Court stated that the central issue in deciding the Motion is whether the November 20, 2012, searches were constitutional. See Aug. 19, 2014 Tr. at 375:23-25 (Court). The Court explained that it was inclined to think “that the Constitution doesn’t put the restrictions . . . on the officers’ search methods as strictly as the defendant is advancing.” Aug. 19, 2014 Tr. at 375:25-376:3 (Court). The Court stated that, if the November 20, 2012, searches were valid, the searches that Nishida conducted pursuant to the Second Warrant would be upheld under “about two or three doctrines.” Aug. 19, 2014 Tr. at 376:6 (Court). The Court said that, accordingly, it was skeptical that it would grant the Motion. See Aug. 19, 2014 Tr. at 376:7-8 (Court).

#### **RELEVANT FOURTH AMENDMENT LAW**

The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” U.S. Const. amend. IV. Fourth Amendment rights are enforceable against state actors through the Due Process Clause of the Fourteenth Amendment to the Constitution of the United States. See Mapp v. Ohio, 367 U.S. 643, 655 (1961); United States v. Rodriguez-Rodriguez, 550 F.3d 1223, 1225 n.1 (10th Cir.

2008)(“[T]he Fourth Amendment applies against state law enforcement officials as incorporated through the Due Process Clause of the Fourteenth Amendment.”). “Not all searches require a warrant. The hallmark of the Fourth Amendment is reasonableness.” United States v. Harmon, 785 F. Supp. 2d at 1157. See United States v. McHugh, 639 F.3d 1250, 1260 (10th Cir. 2011)(“[T]he ultimate touchstone of the Fourth Amendment is ‘reasonableness.’”)(quoting Brigham City v. Stuart, 547 U.S. 398 (1978)). The Supreme Court of the United States has stated that “searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment -- subject only to a few specifically established and well-delineated exceptions.” Katz v. United States, 389 U.S. 347, 357 (1967)(footnotes omitted).

#### **1. The Fourth Amendment “Standing” Analysis.**

“The Tenth Circuit has referred to the test whether a particular search implicates a defendant’s Fourth Amendment interests -- whether the search violates the defendant’s reasonable privacy expectation -- as one of ‘standing.’” Ysasi v. Brown, CIV 13-0183 JB/CG, 2014 WL 936835, at \*8 (D.N.M. Feb. 28, 2014)(Browning, J.)(citing United States v. Creighton, 639 F.3d 1281, 1286 (10th Cir. 2011)(“The Defendant has the burden of establishing . . . standing, or, in other words, a subjective expectation of privacy in the [item searched] that society is prepared to recognize as reasonable.”); United States v. Poe, 556 F.3d 1113, 1121 (10th Cir. 2009)(“[A] defendant raising a Fourth Amendment challenge must first demonstrate that he has standing to object to the search.”)(citing United States v. Rubio-Rivera, 917 F.2d 1271, 1274 (10th Cir. 1990)); United States v. Shareef, 100 F.3d 1491, 1499 (10th Cir. 1996)(“A Defendant has standing to challenge a search only if he or she has a reasonable expectation of privacy in the area being searched.”)). Accordingly, the Court, following the Tenth Circuit’s

lead, has also referred to this test as one of standing. See, e.g., United States v. Harmon, 785 F. Supp. 2d at 1157 (“Standing requires the defendant to show ‘that he had a subjective expectation of privacy in the premises searched and that society is prepared to recognize that expectation as reasonable.’”)(quoting United States v. Poe, 556 F.3d at 1121). The Supreme Court’s decisions suggest, however, that the “standing” test has now expressly been incorporated into the substantive Fourth Amendment search analysis. See United States v. Sweeney, CR 14-0020, 2014 WL 2514926, at \*2 (E.D. Wis. June 4, 2014)(Adelman, J.) (“Once referred to as ‘standing,’ this requirement is actually part of substantive Fourth Amendment law.”).

In Rakas v. Illinois, 439 U.S. 128 (1978), the Supreme Court disapproved of labeling the inquiry whether a search implicates a defendant’s personal Fourth Amendment interests “as one of standing, rather than simply recognizing it as one involving the substantive question of whether or not the proponent of the motion to suppress had his own Fourth Amendment rights infringed by the search and seizure which he seeks to challenge.” 439 U.S. at 133. Dispensing with this label, the Supreme Court noted:

Had we accepted petitioners’ request to allow persons other than those whose own Fourth Amendment rights were violated by a challenged search and seizure to suppress evidence obtained in the course of such police activity, it would be appropriate to retain Jones’<sup>9</sup> use of standing in Fourth Amendment analysis. Under petitioners’ target theory, a court could determine that a defendant had standing to invoke the exclusionary rule without having to inquire into the substantive question of whether the challenged search or seizure violated the Fourth Amendment rights of that particular defendant. However, having rejected petitioners’ target theory and reaffirmed the principle that the “rights assured by the Fourth Amendment are personal rights, [which] . . . may be enforced by exclusion of evidence only at the instance of one whose own protection was infringed by the search and seizure,” Simmons v. United States, 390 U.S. [377, 389 (1968)] . . . , the question necessarily arises whether it serves any useful analytical purpose to consider this principle a matter of standing, distinct from the merits of a defendant’s Fourth Amendment claim. We can think of no decided

---

<sup>9</sup>Jones v. United States, 362 U.S. 257 (1960), overruled by United States v. Salvucci, 448 U.S. 83 (1980).

cases of this Court that would have come out differently had we concluded, as we do now, that the type of standing requirement discussed in Jones, and reaffirmed today is more properly subsumed under substantive Fourth Amendment doctrine. Rigorous application of the principle that the rights secured by this Amendment are personal, in place of a notion of “standing,” will produce no additional situations in which evidence must be excluded. The inquiry under either approach is the same. But we think the better analysis forthrightly focuses on the extent of a particular defendant’s rights under the Fourth Amendment, rather than on any theoretically separate, but invariably intertwined concept of standing. The Court in Jones, also may have been aware that there was a certain artificiality in analyzing this question in terms of standing because in at least three separate places in its opinion the Court placed that term within quotation marks.

439 U.S. at 138-39 (citations omitted). The Supreme Court emphasized:

[N]othing we say here casts the least doubt on cases which recognize . . . as a general proposition, the issue of standing [generally.] . . . But this Court’s long history of insistence that Fourth Amendment rights are personal in nature has already answered many of these traditional standing inquiries, and we think that definition of those rights is more properly placed within the purview of substantive Fourth Amendment law than within that of standing.

439 U.S. at 139-40. In Minnesota v. Carter, 525 U.S. 83 (1998), the Supreme Court recognized that Rakas v. Illinois put an end to the Fourth Amendment standing analysis as separate from the substantive Fourth Amendment search analysis:

The Minnesota courts analyzed whether respondents had a legitimate expectation of privacy under the rubric of “standing” doctrine, an analysis that this Court expressly rejected 20 years ago in Rakas . . . Central to our analysis [in Rakas v. Illinois] was the idea that in determining whether a defendant is able to show the violation of his (and not someone else’s) Fourth Amendment rights, the “definition of those rights is more properly placed within the purview of substantive Fourth Amendment law than within that of standing.”

525 U.S. at 87-88 (citations omitted). The Supreme Court has, thus, noted that the analysis under either approach -- the substantive Fourth Amendment doctrine that the rights that the Amendment secures are personal versus the separate notion of “standing” -- is the same. Rakas v. Illinois, 439 U.S. at 139.

## 2. Whether a Fourth Amendment Search Occurred.

A court cannot suppress evidence unless the search was a Fourth Amendment search. A Fourth Amendment search occurs either where the government, to obtain information, trespasses on a person's property or where the government violates a person's subjective expectation of privacy that society recognizes as reasonable to collect information. See United States v. Jones, 132 S. Ct. at 947. "[T]he Katz reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test." United States v. Jones, 132 S. Ct. at 947 (emphasis in original)(citing Alderman v. United States, 394 U.S. 165 (1969); Soldal v. Cook Cnty., 506 U.S. 56, 64 (1992)).

### a. Trespass-Based Analysis.

In Florida v. Jardines, the Supreme Court explained that the Fourth Amendment "establishes a simple baseline, one that for much of our history formed the exclusive basis for its protections: When 'the Government obtains information by physically intruding' on persons, houses, papers, or effects, 'a search within the original meaning of the Fourth Amendment' has 'undoubtedly occurred.'" 133 S. Ct. at 1414 (quoting United States v. Jones, 132 S. Ct. at 950 n.3). "[A]n actual trespass," however, "is neither necessary nor sufficient to establish a constitutional violation." United States v. Jones, 132 S. Ct. at 951 n.5 (Scalia, J.)(emphasis omitted)(quoting United States v. Karo, 468 U.S. 705, 713 (1984)). In determining whether a search has occurred, "[t]respass alone does not qualify, but there must be conjoined with that . . . an attempt to find something or to obtain information." United States v. Jones, 132 S. Ct. at 951 n.5. The Supreme Court has also noted that "[p]hysically invasive inspection is simply more intrusive than purely visual inspection." Bond v. United States, 529 U.S. 334, 337 (2000). Moreover, the Supreme Court, in Florida v. Jardines, suggested that the trespass-based



analysis applies only when the trespass occurs in one of the four places or things listed in the Fourth Amendment:

The Fourth Amendment “indicates with some precision the places and things encompassed by its protections”: persons, houses, papers, and effects. The Fourth Amendment does not, therefore, prevent all investigations conducted on private property; for example, an officer may (subject to Katz) gather information in what we have called “open fields” -- even if those fields are privately owned -- because such fields are not enumerated in the Amendment’s text . . . . But when it comes to the Fourth Amendment, the home is first among equals.

133 S. Ct. at 1414.

In United States v. Alabi, 943 F. Supp. 2d 1201 (D.N.M. 2013)(Browning, J.), the Court analyzed whether the Secret Service’s digital scan of electronic information contained in the defendants’ credit and debit cards’ magnetic strips was a Fourth Amendment search under a trespass-based analysis, concluding that it was not, because the Secret Service properly possessed the credit and debit cards, and the additional act of scanning the cards to read the virtual data contained on the strips did not involve a physical intrusion or physical penetration of space. See 943 F. Supp. 2d at 1264-65. The Court noted that, “[e]ven if the Supreme Court were to extend the trespass-based analysis for Fourth Amendment searches to virtual invasions, the Secret Service’s conduct scanning the thirty-one credit and debit cards still would not amount to a Fourth Amendment search,” because the magnetic strip, as opposed to the credit or debit card separately, is not a constitutionally protected area. 943 F. Supp. 2d at 1267-68.

When a law enforcement officer sees only the exterior of a credit or debit card, however, given that the financial institution which issues the card places the same information on the magnetic strip as embossed on the card’s exterior, the only instances in which the information inside the credit or debit card is not information already seen by and known to the officer is when the information has been reencoded for unlawful purposes. In these instances, not only does the person asserting his or her Fourth Amendment right not own or otherwise lawfully possess the information contained inside the card on the magnetic strip, but the person has stolen the information with the intent to use that information to steal further from the person whose information is on the magnetic strip.

Protecting this area from law enforcement search and seizure would thus not further the Fourth Amendment's express purpose of protecting "[t]he right of the people to be secure in *their* persons, houses, papers, and effects . . . ." U.S. Const. amend IV.

943 F. Supp. 2d at 1273 (alteration in original).

**b. Katz v. United States' Reasonable-Expectation-of-Privacy Test Remains Good Law.**

The Court has noted that, in light of the Supreme Court's recent decisions in Florida v. Jardines and United States v. Jones, both of which Justice Scalia wrote for the majority, and both of which analyze whether government conduct constituted a Fourth Amendment search using the trespass-based approach, "the question arises whether the Katz v. United States reasonable-expectation-of-privacy test is still good law." United States v. Alabi, 943 F. Supp. 2d at 1242 (citing Minnesota v. Carter, 525 U.S. at 97-98 (Scalia, J., concurring)). Justice Scalia has consistently criticized this "notoriously unhelpful test":

In my view, the only thing the past three decades have established about the Katz test (which has come to mean the test enunciated by Justice Harlan's separate concurrence in Katz . . . ) is that, unsurprisingly, those "actual (subjective) expectation[s] of privacy" "that society is prepared to recognize as 'reasonable,'" bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable. When that self-indulgent test is employed (as the dissent would employ it here) to determine whether a "search or seizure" within the meaning of the Constitution has *occurred* (as opposed to whether that "search or seizure" is an "unreasonable" one), it has no plausible foundation in the text of the Fourth Amendment. That provision did not guarantee some generalized "right of privacy" and leave it to this Court to determine which particular manifestations of the value of privacy "society is prepared to recognize as 'reasonable.'" Rather, it enumerated ("persons, houses, papers, and effects") the objects of privacy protection to which the *Constitution* would extend, leaving further expansion to the good judgment, not of this Court, but of the people through their representatives in the legislature.

Minnesota v. Carter, 525 U.S. at 97-98 (Scalia, J., concurring)(emphasis in original)(citations omitted). In both United States v. Jones and Florida v. Jardines, however, Justice Scalia, writing for the majority, never stated that the Supreme Court was substituting the trespass-based analysis

for Katz v. United States’ reasonable-expectation-of-privacy analysis. Rather, his majority opinions asserted that the Katz v. United States reasonable-expectation-of-privacy analysis added to the trespass-based analysis. See Florida v. Jardines, 133 S. Ct. at 1417 (“The Katz reasonable-expectations test ‘has been *added to*, not *substituted for*,’ the traditional property-based understanding of the Fourth Amendment.” (emphasis in original))(quoting United States v. Jones, 132 S. Ct. at 952). The Court concluded in United States v. Alabi that, “as the Supreme Court now stands, Justices Alito, Breyer, Kagan, Ginsburg, and Sotomayor still adhere to application of the Katz v. United States reasonable-expectation-of-privacy Fourth Amendment analysis, at least as a possible approach alongside of the trespass-based approach.” 943 F. Supp. 2d at 1243.

In June, 2013, Justice Scalia dissented from the Supreme Court’s decision in Maryland v. King, 133 S. Ct. 1958 (2013), in which the Supreme Court held that “DNA identification of arrestees is a reasonable search that can be considered part of a routine booking procedure,” 133 S. Ct. at 1980. Justice Scalia criticized the majority opinion for analogizing DNA testing to taking an arrestee’s photograph by citing to Katz v. United States and pointing out that “we have never held that merely taking a person’s photograph invades any recognized ‘expectation of privacy.’” Maryland v. King, 133 S. Ct. at 1986 (Scalia, J., dissenting). Justice Scalia also pointed out that a person’s “privacy-related concerns” in his or her body are weighty:

We are told that the “privacy-related concerns” in the search of a home “are weighty enough that the search may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee.” But why are the “privacy-related concerns” not also “weighty” when an intrusion into the *body* is at stake? (The Fourth Amendment lists “persons” *first* among the entities protected against unreasonable searches and seizures.).

Maryland v. King, 133 S. Ct. at 1982 (Scalia J., dissenting)(emphasis in original). Justice Scalia also suggested that the Founders would have shared these privacy-related concerns:

Today's judgment will, to be sure, have the beneficial effect of solving more crimes; then again, so would the taking of DNA samples from anyone who flies on an airplane (surely the Transportation Security Administration needs to know the "identity" of the flying public), applies for a driver's license, or attends a public school. Perhaps the construction of such a genetic panopticon is wise. But I doubt that the proud men who wrote the charter of our liberties would have been so eager to open their mouths for royal inspection.

Maryland v. King, 133 S. Ct. at 1989 (Scalia J., dissenting). The Court, therefore, concludes that Justice Scalia and the Supreme Court may still rely on a person's privacy expectation when determining whether a search is reasonable for Fourth Amendment purposes, although Justice Scalia may not turn to the expectations prong until after he runs the facts through the trespass prong.

**c. Katz v. United States' Reasonable-Expectations-of-Privacy Analysis.**

"Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted." Rakas v. Illinois, 439 U.S. at 133-34 (quoting Alderman v. United States, 394 U.S. at 174). "A district court cannot suppress evidence unless the movant proves that a search implicates *personal* Fourth Amendment interests." United States v. Jones, 44 F.3d 860, 871 (10th Cir. 1995)(emphasis in original). "[N]o interest legitimately protected by the Fourth Amendment' is implicated by governmental investigative activities unless there is an intrusion into a zone of privacy, into 'the security a man relies upon when he places himself or his property within a constitutionally protected area.'" United States v. Miller, 425 U.S. 435, 440 (1976)(Hoffa v. United States, 385 U.S. 293, 301-02 (1966)). The Tenth Circuit has, thus, noted that "[a]n illegal search or seizure only harms those with legitimate expectations of privacy in the premises searched." United States v. Jones, 44 F.3d at 871 (citing United States v. Roper, 918 F.2d 885, 886-87 (10th Cir. 1990)). Thus, "[t]he proper inquiry" to determine whether a search implicates a defendant's Fourth Amendment interests still depends,

after conducting a trespass-based analysis, on “whether the defendant had an expectation of privacy in the place searched and whether that expectation was objectively reasonable.” Kerns v. Bd. of Comm’rs of Bernalillo Cnty., 888 F. Supp. 2d 1176, 1219 (D.N.M. 2012)(Browning, J.) abrogated on other grounds as recognized in Ysasi v. Brown, 2014 WL 936835, at \*9 n.24.

“Official conduct that does not ‘compromise any legitimate interest in privacy’ is not a search subject to the Fourth Amendment.” Illinois v. Caballes, 543 U.S. at 409 (quoting United States v. Jacobsen, 466 U.S. at 123). The Supreme Court has, thus, recognized that, rather than determining whether law enforcement conduct was a search, it sometimes proves easier to “assess[] when a search is not a search.” Kyllo v. United States, 533 U.S. at 32.

In assessing when a search is not a search, we have applied somewhat in reverse the principle first enunciated in Katz v. United States. Katz involved eavesdropping by means of an electronic listening device placed on the outside of a telephone booth -- a location not within the catalog (“persons, houses, papers, and effects”) that the Fourth Amendment protects against unreasonable searches. We held that the Fourth Amendment nonetheless protected Katz from the warrantless eavesdropping because he “justifiably relied” upon the privacy of the telephone booth. As Justice Harlan’s oft-quoted concurrence described it, a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.

Kyllo v. United States, 533 U.S. at 32-33. The Supreme Court, thus, articulated the Katz v. United States rule -- which Professor Wayne R. LaFave has noted is “somewhat inaccurately stated as the ‘reasonable expectation of privacy’ test,” Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment § 2.1(b), at 435 (4th ed., 2004) -- which posits: “[A] Fourth Amendment search does not occur . . . unless ‘the individual manifested a subjective expectation of privacy in the object of the challenged search,’ and ‘society [is] willing to recognize that expectation as reasonable.’” Kyllo v. United States, 533 U.S. at 33 (emphasis in original)(quoting California v. Ciraolo, 476 U.S. 207, 211 (1986)).

A “reasonable expectation of privacy” is “said to be an expectation ‘that has a source

outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.” United States v. Jones, 132 S. Ct. at 951. See United States v. Harmon, 785 F. Supp. 2d at 1157 (“To decide whether a reasonable expectation of privacy exists, courts consider concepts of real or personal property law . . . .”). In analyzing whether an expectation of privacy is reasonable in the Fourth Amendment context based on property law, “arcane distinctions developed in property and tort law between guests, licensees, invitees, and the like, ought not to control.” Rakas v. Illinois, 439 U.S. at 143 & n.12. Although ownership or lawful possession is not determinative under the Katz v. United States reasonable-expectation-of-privacy test, it is often a dispositive factor; because the Fourth Amendment is a personal right, a defendant bears the burden of demonstrating “that he gained possession [of the area searched] from the owner or someone with the authority to grant possession.” United States v. Arango, 912 F.2d 441, 445-46 (10th Cir. 1990).

**i. Subjective Expectation of Privacy.**

A defendant maintains a subjective expectation of privacy when he or she “has shown that ‘he sought to preserve something as private.’” Ysasi v. Brown, 2014 WL 936835, at \*8 (quoting Bond v. United States, 529 U.S. at 338). Thus, there is no reasonable expectation of privacy in otherwise private information disclosed to a third party. “[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.” Katz v. United States, 389 U.S. at 351. The Supreme Court has noted:

This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third

party will not be betrayed.

United States v. Miller, 425 U.S. at 443.

The Supreme Court has recognized, however, that subjective expectations of privacy do not always coincide with the interests that the Fourth Amendment is universally thought to protect. In Smith v. Maryland, for instance, the Supreme Court identified situations in which it would not follow the subjective approach:

Situations can be imagined, of course, in which Katz' two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation or [sic] privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. In such circumstances, where an individual's subjective expectations had been "conditioned" by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a "legitimate expectation of privacy" existed in such cases, a normative inquiry would be proper.

Smith v. Maryland, 442 U.S. at 740 n.5. Most recently, in United States v. Jones, Justice Sotomayor commented that, given the reality of technology in the twenty-first century, it may no longer be sound to universally hold to the third-party disclosure rule to determine whether a subjective expectation of privacy exists:

[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice Alito notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," and

perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

132 S. Ct. at 957 (Sotomayor, J., concurring)(citations omitted). The Court notes, however, that, regardless what the Supreme Court decides to do with social media on the internet, only the most ignorant or gullible think that what they post on the internet is or remains private. See United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012)(Pauley, J.)(holding that a person posting to his Facebook profile had “no justifiable expectation that his ‘friends’ would keep his profile private”).

**ii. Privacy Expectation That Society Is Prepared to Recognize as Reasonable.**

Under the second step of Katz v. United States’ reasonable-expectation-of-privacy approach, courts must determine “whether society is prepared to recognize that [subjective privacy] expectation as objectively reasonable.” United States v. Ruiz, 664 F.3d 833, 838 (10th Cir. 2012)(United States v. Allen, 235 F.3d 482, 489 (10th Cir. 2000)). The Supreme Court has cautioned: “The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, however well justified, that certain facts will not come to the attention of the authorities.” United States v. Jacobsen, 466 U.S. 109, 122 (1984). “Determining whether society would view the expectation as objectively reasonable turns on whether the government’s intrusion infringes on a legitimate interest, based on the values that the Fourth Amendment protects.” United States v. Alabi, 943 F. Supp. 2d at 1247 (citing California v. Ciraolo, 476 U.S. at 212 (explaining that “[t]he test of



legitimacy is not whether the individual chooses to conceal assertedly ‘private’ activity,” but instead “whether the government’s intrusion infringes upon the personal and societal values protected by the Fourth Amendment”). This second factor of the Katz v. United States reasonable-expectation-of-privacy analysis developed from Justice Harlan’s “attempt to give content to the word ‘justifiably’ in the majority’s assertion that eavesdropping on Katz was a search because it ‘violated the privacy upon which he justifiably relied while using the telephone booth.’” LaFave, § 2.1(d), at 439 (quoting Katz v. United States, 389 U.S. at 353). Thus, whether society will recognize a certain expectation of privacy does not turn on whether the hypothetical reasonable person would hold the same expectation of privacy, but rather on whether the expectation of privacy is justified or legitimate. The Supreme Court has provided that, while no single factor determines legitimacy, whether society recognizes a privacy interest as reasonable is determined based on our societal understanding regarding what deserves protection from government invasion:

No single factor determines whether an individual legitimately may claim under the Fourth Amendment that a place should be free of government intrusion not authorized by warrant. In assessing the degree to which a search infringes upon individual privacy, the Court has given weight to such factors as the intention of the Framers of the Fourth Amendment, the uses to which the individual has put a location, and our societal understanding that certain areas deserve the most scrupulous protection from government invasion.

Oliver v. United States, 466 U.S. at 177-78 (citations omitted).

The Supreme Court has held that “[o]fficial conduct that does not ‘compromise any legitimate interest in privacy’ is not a search subject to the Fourth Amendment.” Illinois v. Caballes, 543 U.S. at 409 (quoting United States v. Jacobsen, 466 U.S. at 123). In United States v. Place, the Supreme Court held that the “canine sniff” of a drug-sniffing dog does “not constitute a ‘search’ within the meaning of the Fourth Amendment.” United States v. Place, 462

U.S. at 707. The case arose when law enforcement seized the luggage of an airline passenger and transported it to another location, where a drug-sniffing dog could sniff it. See 462 U.S. at 699. The drug-sniffing dog alerted the officers that drugs were in the luggage, the officers obtained a search warrant, and, upon opening the bags, the officers found over one-thousand grams of cocaine. See 462 U.S. at 699. While recognizing that a person has a reasonable expectation of privacy in the contents of his or her luggage, the Supreme Court held that the dog's sniff test was not a Fourth Amendment search and emphasized the unique nature of the investigative technique, which could identify only criminal activity:

We have affirmed that a person possesses a privacy interest in the contents of personal luggage that is protected by the Fourth Amendment. A "canine sniff" by a well-trained narcotics detection dog, however, does not require opening the luggage. It does not expose noncontraband items that otherwise would remain hidden from public view, as does, for example, an officer's rummaging through the contents of the luggage. Thus, the manner in which information is obtained through this investigative technique is much less intrusive than a typical search. Moreover, the sniff discloses only the presence or absence of narcotics, a contraband item. Thus, despite the fact that the sniff tells the authorities something about the contents of the luggage, the information obtained is limited. This limited disclosure also ensures that the owner of the property is not subjected to the embarrassment and inconvenience entailed in less discriminate and more intrusive investigative methods.

In these respects, the canine sniff is *sui generis*. We are aware of no other investigative procedure that is so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure. Therefore, we conclude that the particular course of investigation that the agents intended to pursue here -- exposure of respondent's luggage, which was located in a public place, to a trained canine -- did not constitute a "search" within the meaning of the Fourth Amendment.

United States v. Place, 462 U.S. at 707.

In United States v. Jacobsen, the Supreme Court extended this holding to the chemical field test of a white powdery substance to reveal that the substance was cocaine. See 466 U.S. at 122-24. A Federal Express employee and supervisor opened a damaged package, and exposed

four zip-lock plastic bags containing six and one-half ounces of white powder. See 466 U.S. at 111. They then called the Drug Enforcement Agency and repacked the contents in the original packaging before they provided the package to the DEA officers. See 466 U.S. at 111. When the agents arrived, the agents removed the exposed plastic bags from the broken package, opened each of the four bags, and field-tested the white powder, identifying the powder as cocaine. See 466 U.S. at 111-12. The Supreme Court first held that removal of the plastic bags from the tubes and the agent's visual inspection were not Fourth Amendment searches:

The removal of the plastic bags from the tube and the agent's visual inspection of their contents enabled the agent to learn nothing that had not previously been learned during the private search. It infringed no legitimate expectation of privacy and hence was not a "search" within the meaning of the Fourth Amendment.

466 U.S. at 120 (footnote omitted). The Supreme Court noted: "The question remains whether the additional intrusion occasioned by the field test, which had not been conducted by the Federal Express agents and therefore exceeded the scope of the private search, was an unlawful 'search' or 'seizure' within the meaning of the Fourth Amendment." United States v. Jacobsen, 466 U.S. at 122. The Supreme Court, relying on United States v. Place, held that the additional digital scan of the white substance was not a Fourth Amendment search, because the test discloses only whether the substance is cocaine and "nothing [else] of special interest":

The field test at issue could disclose only one fact previously unknown to the agent -- whether or not a suspicious white powder was cocaine. It could tell him nothing more, not even whether the substance was sugar or talcum powder. We must first determine whether this can be considered a "search" subject to the Fourth Amendment -- did it infringe an expectation of privacy that society is prepared to consider reasonable?

. . . .

A chemical test that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy. This conclusion is not dependent on the result of any particular test. It is probably safe to assume

that virtually all of the tests conducted under circumstances comparable to those disclosed by this record would result in a positive finding; in such cases, no legitimate interest has been compromised. But even if the results are negative -- merely disclosing that the substance is something other than cocaine -- such a result reveals nothing of special interest. Congress has decided -- and there is no question about its power to do so -- to treat the interest in “privately” possessing cocaine as illegitimate; thus governmental conduct that can reveal whether a substance is cocaine, and no other arguably “private” fact, compromises no legitimate privacy interest.

. . . .

Here, as in Place, the likelihood that official conduct of the kind disclosed by the record will actually compromise any legitimate interest in privacy seems much too remote to characterize the testing as a search subject to the Fourth Amendment.

United States v. Jacobsen, 466 U.S. at 122-24.

Most recently, where a “dog sniff was performed on the exterior of respondent’s car while he was lawfully seized for a traffic violation,” the Supreme Court, again relying on United States v. Place and also on United States v. Jacobsen, held that “[a]ny intrusion on respondent’s privacy expectations does not rise to the level of a constitutionally cognizable infringement.” Illinois v. Caballes, 543 U.S. at 409.<sup>10</sup> The Supreme Court reasoned that the dog sniff in Illinois v. Caballes fell squarely in line with the series of cases holding “that any interest in possessing contraband cannot be deemed ‘legitimate,’ and th[at], governmental conduct that *only* reveals the possession of contraband ‘compromises no legitimate privacy interests.’” 543 U.S. at 408 (quoting United States v. Jacobsen, 466 U.S. at 123)(emphasis in original). The Supreme Court explained: “This is because the expectation ‘that certain facts will not come to the attention of the authorities’ is not the same as an interest in ‘privacy that society is prepared to consider

---

<sup>10</sup>The Honorable John Paul Stevens, former Associate Justice of the Supreme Court, penned the majority’s opinion in Illinois v. Caballes. Out of the current Supreme Court Justices, Justices Scalia, Kennedy, Thomas, and Breyer joined Justice Stevens’ majority opinion, while Justice Ginsburg dissented. See 543 U.S. at 405.

reasonable,” 543 U.S. at 408-09 (quoting United States v. Jacobsen, 466 U.S. at 122). The Supreme Court in Illinois v. Caballes noted that its decision was consistent with Kyllo v. United States, as the thermal imaging device in Kyllo v. United States could detect lawful, “intimate details” in a home:

This conclusion is entirely consistent with our recent decision that the use of a thermal-imaging device to detect the growth of marijuana in a home constituted an unlawful search. Kyllo v. United States, 533 U.S. 27 . . . (2001) . . . . Critical to that decision was the fact that the device was capable of detecting lawful activity -- in that case, intimate details in a home, such as “at what hour each night the lady of the house takes her daily sauna and bath.” Id., at 38 . . . . The legitimate expectation that information about perfectly lawful activity will remain private is categorically distinguishable from respondent’s hopes or expectations concerning the nondetection of contraband in the trunk of his car. A dog sniff conducted during a concededly lawful traffic stop that reveals no information other than the location of a substance that no individual has any right to possess does not violate the Fourth Amendment.

Illinois v. Caballes, 543 U.S. at 409-10.

In United States v. Alabi, the defendants possessed thirty-one credit and debit cards, “many of them in their own names, several of which had information on the magnetic strips that related to persons other than the Defendants.” 943 F. Supp. 2d at 1275. The Court reluctantly accepted the defendants’ assertion that they “subjectively intended not to disclose this information to a third party -- i.e., intended not to use the cards,” 943 F. Supp. 2d at 1275, but determined that “a privacy expectation in the account information stored on credit and debit cards’ magnetic strips -- separate and beyond the credit and debit cards themselves -- is not objectively reasonable,” 943 F. Supp. 2d at 1280. The Court explained that the Secret Service’s scan of the cards’ magnetic strips “reveals only the same information revealed in a private search when the card is used as intended,” and, further, that, even if the cards had never been used, the scan “discloses only information known by viewing the outside of the card, or information that the cards and account information are possessed unlawfully . . . .” 943 F. Supp. 2d at 1281.

Noting the Supreme Court's decision in Rakas v. Illinois, in which the Supreme Court "reasoned that society is not prepared to recognize as reasonable an expectation of privacy in a burglar robbing a summer cabin during the offseason," the Court concluded that society would not recognize "as reasonable a privacy expectation which, at least in contemporary society, would benefit only criminals." 943 F. Supp. 2d at 1287.

### **3. Search Warrants Require Probable Cause.**

"The Supreme Court requires that a magistrate judge be provided information sufficient to determine the existence of probable cause before he or she issues a warrant." United States v. Romero, 743 F. Supp. 2d 1281, 1302 (D.N.M. 2010)(Browning, J.), aff'd, 749 F.3d 900 (10th Cir. 2014)(citing Illinois v. Gates, 462 U.S. 213, 239 (1983)). Probable cause requires "more than mere suspicion but less evidence than is necessary to convict." United States v. Burns, 624 F.2d 95, 99 (10th Cir. 1980). To establish probable cause to justify a search of a home, an affidavit in support of a search warrant "must contain facts sufficient to lead a prudent person to believe that a search would uncover contraband or evidence of criminal activity." United States v. Danhauer, 229 F.3d 1002, 1006 (10th Cir. 2000). "Probable cause undoubtedly requires a nexus between suspected criminal activity and the place to be searched." United States v. Corral-Corral, 899 F.2d 927, 937 (10th Cir. 1990). The task of the magistrate judge issuing the search warrant "is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the veracity and basis of knowledge of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." United States v. Reed, 195 F. App'x 815, 821 (10th Cir. 2006)(unpublished)(quoting Illinois v. Gates, 462 U.S. at 238). See United States v. Glover, 104 F.3d 1570, 1578 (10th Cir. 1997)(finding that, in determining whether an affidavit

supports a finding of probable cause, the court must review the affidavit as a whole and look to the totality of the information contained therein). In making his or her determination, the Magistrate Judge “may draw reasonable inferences from the material provided in the warrant application.” United States v. Rowland, 145 F.3d 1194, 1205 (10th Cir. 1998).

“A reviewing court should accord great deference to a magistrate’s determination of probable cause.” United States v. Reed, 195 F. App’x at 822. The court’s duty is “simply to ensure that the magistrate had a substantial basis for . . . conclud[ing] that probable cause existed.” Illinois v. Gates, 462 U.S. at 236, 238-39. This deference is appropriate to further the Fourth Amendment’s strong preference for warrants. See Massachusetts v. Upton, 466 U.S. 727, 733 (1984); United States v. Ventresca, 380 U.S. 102, 105-106 (1965)(“An evaluation of the constitutionality of a search warrant should begin with the rule that the informed and deliberate determinations of magistrates empowered to issue warrants . . . are to be preferred over the hurried action of office[r]s”). Because of the strong preference for warrants, “in a doubtful or marginal case a search under a warrant may be sustainable where without one it would fall.” United States v. Ventresca, 380 U.S. at 106.

“The deference accorded a magistrate judge’s probable cause determination, however, is not boundless.” United States v. Alabi, 943 F. Supp. 2d 1201, 1253 (D.N.M. 2013)(Browning, J.)(citing United States v. Leon, 468 U.S. 897, 914 (1984)). The court should not defer to a magistrate judge’s probable-cause determination where there is no substantial basis for concluding that the affidavit in support of the warrant established probable cause. See United States v. Danhauer, 229 F.3d at 1006. Specifically, the court should not defer to a magistrate judge’s probable-cause determination if it “is a mere ratification of the bare conclusions or ‘hunches’ of others or where it involves an improper analysis of the totality of the

circumstances.” United States v. Reed, 195 F. App’x at 822 (citing United States v. Leon, 468 U.S. at 915; Massachusetts v. Upton, 466 U.S. at 734; Illinois v. Gates, 462 U.S. at 239).

#### **4. Search Warrants Require Particularity.**

The Fourth Amendment commands that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. The Supreme Court has explained that the “manifest purpose” of the particularity requirement is “to prevent general searches.” Maryland v. Garrison, 480 U.S. 79, 84 (1987). “By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.” Maryland v. Garrison, 480 U.S. at 84. Moreover, a particular warrant “assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search.” United States v. Chadwick, 433 U.S. 1, 9 (1977)(citations omitted). See also Illinois v. Gates, 462 U.S. at 236 (“[P]ossession of a warrant by officers conducting an arrest or search greatly reduces the perception of unlawful or intrusive police conduct.”).

The Tenth Circuit has cautioned that “the modern development of the personal computer and its ability to store and intermingle a huge array of one’s personal papers in a single place increases law enforcement’s ability to conduct a wide-ranging search into a person’s private affairs, and accordingly makes the particularity requirement that much more important.” United States v. Otero, 563 F.3d at 1132 (citations omitted). Consequently, the Tenth Circuit has struck down search warrants seeking electronically stored information (“ESI”) for lack of particularity where the warrant fails to adequately identify the objects of the search. In United States v.



Riccardi, for example, the Tenth Circuit held a warrant invalid where it permitted a search of “any and all information, data, devices, programs, and other materials” and did not state the crime for which the evidence was sought. 405 F.2d at 863. In Mink v. Knox, the Tenth Circuit similarly rejected a warrant that authorized a search of “all computer and non-computer equipment and written materials in [the defendant’s] house.” 613 F.3d 995, 1011 (10th Cir. 2010). To satisfy the particularity requirement, a search warrant seeking electronically stored information must be limited “either to evidence of specific federal crimes or to specific types of material.” United States v. Christie, 717 F.3d at 1165 (alteration in original)(citations omitted)(internal quotation marks omitted). See, e.g., United States v. Brooks, 427 F.3d at 1252-53 (10th Cir. 2005)(finding warrant valid where it authorized search of computers and disks “for evidence of child pornography”); Davis v. Gracey, 111 F.3d 1472, 1479-80 (10th Cir. 1997)(finding warrant valid where it directed officers to seize equipment pertaining to the distribution or display of pornographic materials in violation of a specific state law).

Recognizing the inherent complexity and unpredictability of ESI searches, however, the Tenth Circuit has never required a search warrant to specify the manner in which law enforcement officers must conduct a search for ESI. See United States v. Brooks, 427 F.3d at 1251 (“The Tenth Circuit has never required warrants to contain a particularized computer search strategy.”). Instead, the Tenth Circuit has recognized:

It is unrealistic to expect a warrant to prospectively restrict the scope of a search by directory, filename or extension or to attempt to structure search methods -- that process must remain dynamic. While file or directory names may sometimes alert one to the contents (e.g., “Russian Lolitas,” “meth stuff,” or “reagents”), illegal activity may not be advertised even in the privacy of one’s personal computer -- it could well be coded or otherwise disguised. The directory structure might give hints as to an effective search strategy, but could just as well be misleading and most often could not effectively, or even reasonably, be described or limited in a warrant. Keyword searches may be useful in locating suspect files, but not always. . . . In summary, it is folly for a search warrant to

attempt to structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objectives. . . . [I]n the end, there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders, and that is true whether the search is of computer files or physical files.

United States v. Burgess, 576 F.3d 1092-1093 (footnotes omitted)(citations omitted).

## **5. The Plain-View Exception.**

The Supreme Court has held that the Fourth Amendment's prohibition on unreasonable searches and seizures does not implicate what a person knowingly exposes to the public in plain view. See Katz v. United States, 389 U.S. at 351 ("What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."). Evidence which is recovered during "a truly cursory inspection -- one that involves merely looking at what is already exposed to view, without disturbing it -- is not a 'search' for Fourth Amendment purposes, and therefore does not even require reasonable suspicion." Arizona v. Hicks, 480 U.S. 321, 328 (1987). See United States v. Nicholson, 144 F.3d 632, 636 (10th Cir. 1998)("[A] visual inspection of that which is in plain view does not constitute a search.")(citing Arizona v. Hicks, 480 U.S. at 328). Evidence or items of contraband discovered in plain view by an officer who is lawfully on the premises are thus admissible as evidence regardless whether the officer was executing a valid search warrant. See Georgia v. Randolph, 547 U.S. 103, 137 (2006); United States v. Romero, 743 F. Supp. 2d at 1307 ("An officer, therefore, does not violate a person's Fourth Amendment rights if the officer is not executing a search warrant, but discovers evidence in plain view, so long as the officer is lawfully on the premises.").

There are three requirements to justify the warrantless seizure of evidence in plain view: "(i) the officer did not violate the Fourth Amendment in arriving at the place from which the evidence could be plainly viewed; (ii) the item's incriminating character is immediately

apparent; and (iii) the officer has a lawful right of access to the object itself.” United States v. Morales-Ortiz, 376 F. Supp. 2d 1131, 1139 (D.N.M. 2004)(Browning, J.)(citing Horton v. California, 496 U.S. 128, 136-37 (1990)).

The plain-view exception does not constrain officers to viewing the evidence with their bare eyes or from a particular position. For example, the Supreme Court has held that “the use of artificial means to illuminate a darkened area simply does not constitute a search, and thus triggers no Fourth Amendment protection.” Texas v. Brown, 460 U.S. 730, 740 (1983)(plurality opinion)(citations omitted). The Court reached a similar conclusion in United States v. Villaba, CR 13-0664 JB, 2013 WL 4782206 (D.N.M. Aug. 21, 2013)(Browning, J.). In that case, an officer used a flashlight to examine the underside of a toy truck and was able to view a plastic bag containing methamphetamine through the slits in the truck’s underside. See United States v. Villaba, 2013 WL 4782206, at \*40. The Court found that the plain-view exception applied, because:

First, . . . Villaba consented to the visual examination and [the officer] also had reasonable suspicion to examine the truck in that manner. Second, based on [the officer]’s reasonable suspicion that the truck contained narcotics, and his experience with narcotics in toys and in baggies, the incriminating character of the taped bag that he saw inside of the slits on the toy truck’s underside was immediately apparent. Third, given either Villaba’s consent or [the officer]’s suspicion, “the officer had a lawful right of access to the object itself.” United States v. Morales-Ortiz, 376 F. Supp. 2d at 1139. Although [the officer] used a flashlight to see the bag inside the truck, given the Supreme Court’s guidance that “the use of artificial means to illuminate a darkened area simply does not constitute a search, and thus triggers no Fourth Amendment protection,” Texas v. Brown, 460 U.S. at 740, the flashlight does not affect the constitutionality of [the officer]’s otherwise lawful search. Thus, once [the officer] viewed the packaging, the incriminating nature of which was immediately apparent, in plain view from where he had a lawful right to be, Walsh had the lawful ability to seize the evidence.

United States v. Villaba, 2013 WL 4782206, at \*40.

The Tenth Circuit has also noted that “an officer may ‘change his position’ and ‘bend

down at an angle’ to see what is inside a car, because ‘there is no reason why an officer should be precluded from observing what would be entirely visible to him as a private citizen.’” United States v. Gonzalez-Acosta, 989 F.2d 384, 387 (10th Cir. 1993)(alterations omitted)(quoting Texas v. Brown, 460 U.S. at 740). Moreover, the Tenth Circuit has held that, “when a container is ‘not closed, or transparent, or when its distinctive configuration proclaims its contents, the container[’s] . . . contents can be said to be in plain view.’” United States v. Corral, 970 F.2d 719, 725 (10th Cir. 1992)(original alterations omitted)(quoting United States v. Donnes, 947 F.2d 1430, 1436 (10th Cir. 1991)). Additionally, “where the police already possess knowledge approaching certainty as to the contents of the container, the search of the container does not unreasonably infringe upon the individual interest in preserving the privacy of those contents.” United States v. Corral, 970 F.2d at 725-26.

#### **RELEVANT LAW ON THE EXCLUSIONARY RULE**

“When evidence is obtained in violation of a person’s constitutional rights, the government is prohibited from using that evidence in a criminal prosecution of that person.” United States v. Villaba, 2013 WL 4782206, at \*27 (citing United States v. Calandra, 414 U.S. 338, 347 (1974)) (“Under this rule, evidence obtained in violation of the Fourth Amendment cannot be used in a criminal proceeding against the victim of the illegal search and seizure.”)). In addition, a court must also suppress any other evidence deemed to be the “fruit of the poisonous tree,” because it is evidence which was discovered as a direct result of the unlawful law enforcement activity. United States v. Olivares-Rangel, 458 F.3d 1104, 1108-09 (10th Cir. 2006). “To suppress evidence that was derived following unlawful activity, the defendant must show that there is a factual nexus between the illegality and the challenged evidence.” United States v. Villaba, 2013 WL 4782206, at \*27 (citing United States v. Olivares-Rangel, 458 F.3d at

1109; United States v. Nava-Ramirez, 210 F.3d at 1131).

“For the exclusionary rule to apply, the defendant must show, by a preponderance of the evidence: (i) a constitutional violation, and (ii) a causal nexus between the violation and the evidence sought to be excluded.” United States v. Villaba, 2013 WL 4782206, at \*27 (citing United States v. Torres-Castro, 470 F.3d 992, 999 (10th Cir. 2006)). Once the defendant makes this showing, if the prosecutor still desires to proffer the challenged evidence, the burden shifts to the prosecution to establish that an exception to the exclusionary rule applies. See United States v. Torres-Castro, 470 F.3d at 999.

### **1. The Good-Faith Exception.**

Recognizing that the “sole purpose” of the exclusionary rule “is to deter future Fourth Amendment violations,” the Supreme Court has held that evidence will not be excluded where the officer who obtained the evidence -- through an unlawful search or seizure -- acted in good faith. United States v. Davis, 131 S. Ct. 2419, 2426 (2011). To determine whether the good-faith exception applies, courts must balance the deterrent effect of excluding the evidence against “the substantial social costs generated by the rule.” 131 S. Ct. at 2427. The Supreme Court has explained that “[t]he basic insight of the Leon line of cases is that the deterrence benefits of exclusion vary with the culpability of the law enforcement conduct at issue.” 131 S. Ct. at 2427. Consequently, “[w]hen the police exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs.” United States v. Davis, 131 S. Ct. at 2438 (citation omitted). By contrast, “[w]hen the police act with an objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence, the deterrence rationale loses much of its force, and exclusion cannot pay its way.” United States v.

Davis, 131 S. Ct. at 2427-28 (citations omitted)(internal quotation marks omitted).

**a. Warrants based on illegally obtained information.**

“When a search is conducted pursuant to a warrant that is based on illegally obtained information, a court is not to blindly apply the good-faith exception.” United States v. Alabi, 943 F. Supp. 2d at 1260. “Instead, the court is to consider the warrant with the illegally obtained information excluded and determine, based on the remaining information, whether probable cause nevertheless existed.” United States v. Alabi, 943 F. Supp. 2d at 1260. If the remaining content of the warrant affidavit establishes probable cause, the search pursuant to that warrant was appropriate, and the evidence need not be excluded:

When a warrant is tainted by some unconstitutionally obtained information, we nonetheless uphold the warrant if there was probable cause absent that information. An affidavit containing erroneous or unconstitutionally obtained information invalidates a warrant if that information was critical to establishing probable cause. If, however, the affidavit contained sufficient accurate or untainted evidence, the warrant is nevertheless valid.

United States v. Sims, 428 F.3d 945, 954 (10th Cir. 2005). See United States v. Cusumano, 83 F.3d 1247, 1250 (10th Cir. 1996)(“In our review, we may disregard allegedly tainted material in the affidavit and ask whether sufficient facts remain to establish probable cause.”); United States v. Snow, 919 F.2d 1458, 1460 (10th Cir. 1990)(“An affidavit containing erroneous or unconstitutionally obtained information invalidates a warrant if that information was critical to establishing probable cause. If, however, the affidavit contained sufficient accurate or untainted evidence, the warrant is nevertheless valid.”). “The apparent rationale for this rule is that one officer cannot execute a warrant ‘in good faith’ if it contains information that he or a fellow officer obtained illegally.” United States v. Alabi, 943 F. Supp. 2d at 1260 (quoting United States v. Herrera, 444 F.3d 1238, 1249 (10th Cir. 2006)).

**b. United States v. Leon.**

In United States v. Leon, the Supreme Court faced the question whether to apply the good-faith exception when a police officer mistakenly thought a warrant, from which he obtained evidence, was supported by probable cause. See 468 U.S. at 905. The Supreme Court noted that excluding this evidence would not deter police misconduct. See 468 U.S. at 918-19. The officer had taken all of the necessary steps to comply with the Fourth Amendment and reasonably thought he warrant, and, thus, his search, was valid. See 468 U.S. at 918-19. The Supreme Court explained that, when a warrant is issued on less than probable cause, the person whose conduct the law wishes to deter is the issuing judge, and that excluding the evidence would not have a significantly deterrent effect on judicial conduct. See 468 U.S. at 916-17. The Supreme Court, thus, concluded that a court need not suppress evidence seized pursuant to a facially valid warrant which later turns out to lack probable cause, as long as police were acting in good-faith reliance on that warrant. See 468 U.S. at 922-23.

“The Tenth Circuit, therefore, now applies the rule that, in cases where the police obtained a warrant but the affidavit supporting the warrant does not establish probable cause, suppression of the evidence found is inappropriate so long as the officers relied on the warrant in good faith.” United States v. Martinez, 696 F. Supp. 2d 1216, 1244 (D.N.M. 2010), aff’d, 643 F.3d 1292 (10th Cir. 2011)(citing United States v. Tuter, 240 F.3d 1292, 1300 (10th Cir. 2001); United States v. Danhauer, 229 F.3d 1002, 1007 (10th Cir. 2000)).

[T]he suppression of evidence obtained pursuant to a warrant should be ordered only in those unusual cases in which exclusion will further the purposes of the exclusionary rule[.] Where an officer acting with objective good faith obtains a search warrant from a detached and neutral magistrate and the executing officers act within its scope, there is nothing to deter.

United States v. Tuter, 240 F.3d at 1298-99. Furthermore, the Tenth Circuit has explained that,

“[u]nder Leon, we presume good-faith when an officer acts pursuant to a warrant unless one of ‘four contexts’ appl[ies].” United States v. Barajas, 710 F.3d 1102, 1110 (10th Cir. 2013).

First, evidence should be suppressed if the issuing magistrate was misled by an affidavit containing false information or information that the affiant would have known was false if not for his “reckless disregard for the truth.” Second, the exception does not apply when the “issuing magistrate wholly abandon[s his] judicial role.” Third, the good-faith exception does not apply when the affidavit in support of the warrant is “so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.” Fourth, the exception does not apply when a warrant is so facially deficient that the executing officer could not reasonably believe it was valid.

United States v. Danhauer, 229 F.3d at 1007 (quoting United States v. Leon, 468 U.S. at 922-23)(citations omitted). See United States v. Perrine, 518 F.3d 1196, 1206-07 (10th Cir. 2008). “If any of these situations is present, the good-faith exception should not be applied, and the evidence should be excluded.” United States v. Romero, 743 F. Supp. 2d at 1316.

### **c. Herring v. United States.**

In Herring v. United States, officers arrested Herring pursuant to an arrest warrant listed in the Dale County, Alabama, warrant database. See 555 U.S. at 137. In the search incident to that arrest, officers found drugs and a gun on Herring’s person. See 555 U.S. at 137. Herring was then indicted on federal gun and drug-possession charges. See 555 U.S. at 138. It turned out, however, that the warrant under which the officers arrested Herring had been recalled, but the database had not been updated to reflect that recall. See 555 U.S. at 138. Asserting that the evidence found during the search was fruit of an unlawful arrest, Herring sought to suppress it. See 555 U.S. at 138. The district court denied Herring’s motion to suppress, and the United States Court of Appeals for the Eleventh Circuit affirmed. See 555 U.S. at 138.

The Supreme Court affirmed the district court’s denial of Herring’s motion to suppress, based primarily on the good-faith exception to the exclusionary rule. See 555 U.S. at 140-46.



The Supreme Court agreed with the Eleventh Circuit that, although the failure of the police to update the warrant database to reflect the fact that Herring's warrant was withdrawn was negligent, it was not reckless or deliberate. See 555 U.S. at 140. The Supreme Court reiterated its holding in Leon: "When police act under a warrant that is invalid for lack of probable cause, the exclusionary rule does not apply if the police acted 'in objectively reasonable reliance' on the subsequently invalidated search warrant." Herring v. United States, 555 U.S. at 142 (citing Leon, 468 U.S. at 922). Tracing the history of cases applying and declining to apply the exclusionary rule, the Supreme Court distilled a general principle: "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." Herring v. United States, 555 U.S. at 144. The Supreme Court further explained that "evidence should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional." Herring v. United States, 555 U.S. at 143. As long as the "police have [not] been shown to be reckless in maintaining [the] warrant system, or to have knowingly made false entries to lay the groundwork for future false arrests," exclusion of evidence is not warranted when the arrest was made on objectively reasonable reliance on a warrant that had been subsequently recalled. Herring v. United States, 555 U.S. at 146.

**c. Davis v. United States.**

In Davis v. United States, the Supreme Court confronted the question of whether to apply the exclusionary rule when police conduct a search in objectively reasonable reliance on binding judicial precedent. See 131 S. Ct. at 2428. At the time of the officer's search, the Supreme Court had not yet decided Arizona v. Gant, 556 U.S. 332 (2009) -- which held that the Fourth

Amendment requires officers to demonstrate a continuing threat to their safety posed by the arrestee or a need to preserve evidence related to the crime of the arrest to justify a warrantless vehicular search incident to arrest. See 556 U.S. at 341-48. The United States Court of Appeals for the Eleventh Circuit had interpreted the Supreme Court's decision in New York v. Belton, 453 U.S. 454 (1981), as establishing a bright-line rule authorizing the search of a vehicle's passenger compartment incident to a recent occupant's arrest. See United States v. Gonzalez, 71 F.3d 819, 825 (11th Cir. 1996). Although the officers' search incident to the defendant's arrest "was in strict compliance with then-binding Circuit law and was not culpable in any way," it was unconstitutional under Arizona v. Gant. See United States v. Davis, 131 S. Ct. at 2428.

The Supreme Court determined that the "acknowledged absence of police culpability dooms [the defendant's] claim." See United States v. Davis, 131 S. Ct. at 2428. The Supreme Court explained that "[p]olice practices trigger the harsh sanction of exclusion only when they are deliberate enough to yield meaningful deterrence, and culpable enough to be worth the price paid by the justice system." United States v. Davis, 131 S. Ct. at 2428 (citations omitted)(internal quotation marks omitted). The Supreme Court stated: "[T]he conduct of the officers here was neither of these things. The officers who conducted the search did not violate [the defendant's] rights deliberately, recklessly, or with gross negligence. Nor does this case involve any recurring or systemic negligence on the part of law enforcement." United States v. Davis, 131 S. Ct. at 2428 (citations omitted)(internal quotation marks omitted). The Supreme Court concluded that, "[u]nless the exclusionary rule is to become a strict-liability regime, it can have no application in this case." United States v. Davis, 131 S. Ct. at 2429.

## **2. The Inevitable Discovery Exception.**

Under the inevitable discovery exception, "illegally obtained evidence may be admitted if

it ‘ultimately or inevitably would have been discovered by lawful means.’” United States v. Christy, 739 F.3d at 540 (quoting Nix v. Williams, 467 U.S. at 444). “The government possesses the burden of proving by a preponderance of the evidence that the evidence at issue would have been discovered without the Fourth Amendment violation.” United States v. Cunningham, 413 F.3d at 1203 (citation omitted). In United States v. Owens, the Tenth Circuit noted that, for the inevitable discovery exception to apply, there must be a “lawful police investigation [that] inevitably would have discovered” the evidence in question. United States v. Owens, 782 F.2d 146, 152 (10th Cir. 1986). Relying on this statement from United States v. Owens, the Court stated in United States v. Christy, 810 F. Supp. 2d 1219 (D.N.M. 2011)(Browning, J.), that the inevitable discovery exception “permits evidence to be admitted if an independent, lawful police investigation inevitably would have discovered it.” 810 F. Supp. 2d at 1274, aff’d, 739 F.3d 534 (10th Cir. 2014)(citations omitted)(internal quotation marks omitted). On appeal, however, the Tenth Circuit clarified that the inevitable discovery exception does not require an independent investigation that would have discovered the evidence in question. See United States v. Christy, 739 F.3d at 540. The Tenth Circuit explained:

In Cunningham and Souza we applied inevitable discovery to situations like the one here -- where there was “one line of investigation that would have led inevitably to the obtaining of a search warrant by independent lawful means but was halted prematurely by a search subsequently contended to be illegal.” Cunningham, 413 F.3d at 1204 n.1. In Cunningham, police searched the defendant’s home after getting his consent. Id. at 1202. The defendant later contested the search, claiming his consent was coerced. Id. We held that even if the search was illegal, the evidence was admissible because the officers “would have obtained a search warrant” if the search had not occurred. Id. at 1205. In Souza, police illegally opened a UPS package that contained drugs. 223 F.3d at 1200, 1202. We held the evidence admissible under inevitable discovery because the officers “would have obtained a warrant” had the illegal search not occurred. Id. at 1206. Thus, our case law does not require a second investigation when the first (and only) investigation would inevitably have discovered the contested evidence by lawful means.

....

Thus, lest there be any doubt, we reaffirm the notion that inevitable discovery requires only that the lawful means of discovery be “independent of the constitutional violation,” Larsen, 127 F.3d at 987, and conclude that a second investigation is not required.

United States v. Christy, 739 F.3d at 540-41.

In United States v. Souza, the Tenth Circuit “set forth the standard for considering whether the inevitable discovery doctrine applies to a warrantless search,” United States v. Cunningham, 413 F.3d at 1203, when “there is no exception to the warrant requirement that could serve as a basis for the inevitable discovery exception,” United States v. Souza, 223 F.3d at 1203. The Tenth Circuit stated that, “a court may apply the inevitable discovery exception only when it has a high level of confidence that the warrant in fact would have been issued and that the specific evidence in question would have been obtained by lawful means.” United States v. Souza, 223 F.3d at 1205. The Tenth Circuit adopted four factors to determine “how likely it is that a warrant would have been issued and that the evidence would have been found pursuant to a warrant:”

1) the extent to which the warrant process has been completed at the time those seeking the warrant learn of the search; 2) the strength of the showing of probable cause at the time the search occurred; 3) whether a warrant ultimately was obtained, albeit after the illegal entry; and 4) evidence that law enforcement agents “jumped the gun” because they lacked confidence in their showing of probable cause and wanted to force the issue by creating a fait accompli.

United States v. Souza, 223 F.3d at 1204 (citing United States v. Cabassa, 62 F.3d 470, 473-74, 473 n.2 (2d Cir. 1995))(citations omitted)(internal quotation marks omitted). Applying the first factor, the Tenth Circuit stated:

[T]he prerequisite to a consideration of the inevitable discovery exception in these cases, steps taken to obtain a warrant prior to the unlawful search, is present in this case. Special Agent Rowden took steps to alert his office that he would be coming back to prepare a warrant for the package and made sure that the affidavit

form would be ready when he got back to his office. Also, the package was specifically placed on the floor behind Detective Sloan for the purpose of obtaining a warrant.

223 F.3d at 1205. Regarding the second factor, the Tenth Circuit stated:

[A]t the time the illegal search occurred, probable cause to believe the package contained contraband was extremely strong. The package itself contained several suspicious characteristics, including all of the openings on the box being heavily taped, the box having been sent through third party shipping, the sender having only used a first name, and the box being solid so that no side of it could be compressed. Moreover, the box was alerted to by a certified narcotics dog, which is itself sufficient to create probable cause.

223 F.3d at 1205-06. The Tenth Circuit noted that a sergeant eventually obtained a search warrant. See 223 F.3d at 1206. Regarding the third factor, the Tenth Circuit stated that, unlike “Cabassa, there is no question . . . concerning the inevitability of discovery of the evidence if the police had obtained a search warrant because the package was secured by the officers and there was no chance that it would not still be there when the warrant actually was issued.” 223 F.3d at 1206. The Tenth Circuit did not reach the fourth factor, but concluded that, although it was

very reluctant to apply the inevitable discovery exception in situations where the government fails to obtain a search warrant and no exception to the warrant requirement exists, in this case the inevitability of discovery of the evidence convince[d] [it] that [the case before it was] one of those occasions when the doctrine should apply.

223 F.3d at 1206.

In United States v. Owens, the Tenth Circuit emphasized the “danger of admitting unlawfully obtained evidence on the strength of some judge’s speculation that it would have been discovered legally anyway.” 782 F.2d at 152-53. The Tenth Circuit considered whether contraband seized without a warrant could still be admitted under the inevitable discovery doctrine. See 782 F.2d at 152-53. Rejecting the United States’ position that the motel maids’ routine cleaning of the defendant’s room for the next occupant would have revealed the

contraband and that, therefore, discovery of the evidence was inevitable, the Tenth Circuit found:

Several factors suggest that motel employees performing routine cleaning may not have inevitably discovered the cocaine. First, if the [motel]’s staff had cleared [the defendant’s] room, they would not necessarily have opened and searched all his luggage and closed containers. In fact, such an intrusion would have been a significant invasion of his privacy. Second, even if the room had been cleared and the white powder inside the closed bag had been discovered by the motel staff, the lack of any police involvement in routine room cleanings suggests that police discovery of the evidence would not have been inevitable. The evidence certainly does not demonstrate that the [motel]’s staff would necessarily have recognized the powder as cocaine or have called the police if they had so recognized it. Finally, absent the unlawful search, [the defendant] might have posted bail on the charge of receiving stolen property and could have returned to his motel room before either the cleaning staff or the police discovered the contraband. Alternatively, a friend could have returned to claim the closed bag.

United States v. Owens, 782 F.2d at 153. “United States v. Owens suggests that courts should be realistic, if not skeptical, when assessing the probability that law-enforcement officers would inevitably have uncovered the challenged evidence through an independent investigation.”

United States v. Martinez, 696 F. Supp. 2d at 1244.

In United States v. Cunningham, the Tenth Circuit “appl[ied] the inevitable discovery doctrine, . . . because [it was] convinced that without Mr. Cunningham’s disputed consent, the warrant to search his house would have been issued and the incriminating evidence would have been discovered.” 413 F.3d at 1205. The Tenth Circuit, in addressing the first factor -- the extent to which the warrant process had been completed at the time those seeking the warrant learn of the search -- stated:

Here, the officers took substantial steps to obtain a warrant before the contested search occurred. The record demonstrates that they had focused their investigation on 1175 and 1179 East 76th Terrace, and had drafted an affidavit to support a search warrant for one of these homes. As a result of their conversation with the AUSA, the officers decided that further surveillance on the two homes was necessary before they specifically selected one to search, and they proceeded to conduct that surveillance immediately. The officers’ actions clearly indicate they took steps to obtain a search warrant and that they intended to obtain the warrant for either 1175 or 1179 East 76th Terrace as soon as possible.

413 F.3d at 1204. Regarding the second factor -- the strength of the showing of probable cause at the time the search occurred -- the Tenth Circuit stated:

The officers also possessed strong probable cause for their search of 1179 East 76th Terrace by the time Mr. Cunningham arrived at the home. Prior to that time, they had acquired background information about the alleged check-writing ring, narrowed their investigation to one residential block, and focused on the two homes sharing a common driveway. The officers' surveillance had uncovered the following additional information: a red car containing two individuals identified earlier in the investigation arrived, parked briefly, and then pulled out from behind 1179 East 76th Terrace; a black pickup truck previously observed in the investigation was stopped containing Mr. Cunningham, who said that he lived at 1179 East 76th Terrace; the residents of 1175 East 76th Terrace told officers that the home next door had been receiving all of the traffic that evening, and the officers ruled out 1175 East 76th Terrace as the location visited by the alleged check supplier; and a gray Blazer previously observed in the investigation was seen parked by 1179 East 76th Terrace. The government thus had sufficient probable cause for a search of 1179 East 76th Terrace at the time of Mr. Cunningham's disputed consent to search his home.

413 F.3d at 1204-1205. Regarding the third factor -- whether a warrant ultimately was obtained, albeit after the illegal entry -- the Tenth Circuit stated: "Moreover, the officers ultimately did obtain a warrant, albeit based in part on information retrieved from inside Mr. Cunningham's home." 413 F.3d at 1205. Regarding the fourth factor -- evidence that the officers "jumped the gun," because they lacked confidence in their showing of probable cause and wanted to force the issue by creating a *fait accompli* -- the Tenth Circuit stated:

There is also no evidence the officers "jumped the gun" due to a lack of confidence about probable cause and out of a desire to force the issue. Instead, the record indicates that the search occurred at the time it did because of the coincidental arrival of Mrs. Cunningham. Her presence on the scene led to a series of events that culminated in her son's release from jail, his return home, and his consent to search. As a result, we are satisfied the government has demonstrated that, as in Souza, but for Mrs. Cunningham's arrival at 1179 East 76th Terrace on the evening of the search, the officers would have obtained a search warrant and the evidence in question would have been found.

413 F.3d at 1205 (citations omitted). The Tenth Circuit, therefore, applied the inevitable

discovery doctrine. See 413 F.3d at 1205.

In United States v. Christy, the Court applied the four United States v. Souza factors and determined that the inevitable discovery exception applied. Regarding the first factor -- the extent to which the warrant process had been completed at the time those seeking the warrant learn of the search -- the Court stated: “The deputies did not take any steps to obtain a warrant before entering Christy’s residence. The United States concedes that they did not attempt to obtain a warrant before entering Christy’s residence. . . . This factor thus weighs against applying the inevitable discovery exception.” 810 F. Supp. 2d at 1275 (citations omitted). As to the second factor -- the strength of the showing of probable cause at the time the search occurred -- the Court concluded:

The Court finds that [Investigator Carvo] had strong probable cause that Christy committed crimes. At the time of the search, Carvo believed he had probable cause for the California crime of unlawful sexual intercourse, because Christy and K.Y. exchanged naked pictures through electronic mail transmissions over the internet and then arranged a meeting in the middle of the night for K.Y. to run away with Christy.

. . . .

Because [the officer] knew that K.Y. and Christy were exchanging naked pictures, “the belief that there was a sexual relationship or sexual interest between the two was reasonable.” Amended Memorandum Opinion and Order at 57. These circumstances are sufficient to form “a reasonable ground for belief of [Christy’s] guilt,” . . . for the California crime of unlawful sexual intercourse.

[The officer] also had strong probable cause for the federal crime of coercion or enticement. Carvo believed that he had probable cause for the federal crime of enticement or coercion, because of Christy’s and K.Y.’s communications through the internet and electronic mail transmissions, because Christy sent K.Y. naked pictures of himself and solicited pictures of K.Y., which showed her breasts, and because cellular telephone evidence shows that Christy traveled across state lines to bring K.Y. to New Mexico.

. . . .

Because [the officer] knew that Christy and K.Y. communicated through



electronic mail transmissions, that Christy sent K.Y. naked pictures of himself and solicited pictures of K.Y., because evidence showed that Christy traveled across state lines with K.Y., and because Carvo had strong probable cause that Christy committed the California crime of unlawful sexual intercourse, Carvo had “a reasonable ground for belief of [Christy’s] guilt,” . . . for the federal crime of coercion or enticement. Because Carvo had strong probable cause for the California crime of unlawful sexual intercourse and for the federal crime of enticement or coercion, this factor weighs in favor of application of the inevitable discovery doctrine.

810 F. Supp. 2d at 1276-78 (brackets in original)(citations omitted). Regarding the third factor, -- whether a warrant ultimately was obtained, albeit after the illegal entry -- the Court held:

The deputies “ultimately did obtain a warrant, albeit based in part on information retrieved” from Littlefield’s actions of peering through a crack in the blinds in Christy’s window, and from the deputies’ entry into Christy’s residence and subsequent interview of Christy. United States v. Cunningham, 413 F.3d at 1205. Although portions of the affidavits supporting the warrants were based on information the Court has found illegally obtained, the affidavits also included information from the California investigation. Although the Tenth Circuit appears to rely on illegally obtained information in its inevitable discovery analysis, the Court does not believe that it can do so. Carvo had strong probable cause that Christy committed California and federal crimes, and Carvo’s probable cause was based on his investigation, and not on any information he learned from the BCSO or from the Albuquerque FBI. . . . Because Carvo had strong probable cause for a California crime and a federal crime, based on information that he learned in his investigation, and not based on information he learned from the BCSO or from the Albuquerque FBI, Carvo would have obtained search warrants that were not based on illegally obtained information. Based upon Carvo’s belief that he had probable cause for both violations of California state law and violations of federal law, he would “have asked [the Bernalillo County Sheriff’s Office (“BCSO”) and/or -- either one -- the FBI to obtain a search warrant for [Christy’s] Albuquerque residence, vehicle, computers, cell phones, things of that nature.” . . . If the BCSO or Albuquerque FBI were not able to obtain a search warrant for these locations, Carvo would have written a federal search warrant himself and come to the District of New Mexico to seek the warrant with himself as the affiant. . . . Carvo is cross designated to acquire both state and federal search warrants. . . . This factor thus weighs in favor of application of the inevitable-discovery doctrine.

United States v. Christy, 810 F. Supp. at 1278-79. As to the fourth factor -- the existence of evidence that the officers jumped the gun because they lacked confidence in their showing of

probable cause and wanted to force the issue by creating a fait accompli -- the Court determined:

There is “no evidence that the officers ‘jumped the gun’ due to a lack of confidence about probable cause and out of a desire to force the issue.” United States v. Cunningham, 413 F.3d at 1205. The record indicates that the search occurred when it did because the deputies believed that they had exigent circumstances to enter Christy’s residence. This factor thus weighs in favor of application of the inevitable discovery doctrine.

United States v. Christy, 810 F. Supp. 2d at 1279. Consequently, the Court applied the inevitable discovery doctrine. See 810 F. Supp. 2d at 1279.

On appeal, the Tenth Circuit affirmed the Court’s decision. See 739 F.3d at 539-544. Addressing the United States v. Souza factors, the Tenth Circuit pointed out that the defendant only challenged the Court’s ruling on factors two and four -- the strength of the probable cause showing when the unlawful search occurred and whether the officers “jumped the gun” to sidestep the warrant requirement. 739 F.3d at 541. Regarding the second factor -- the strength of the showing of probable cause at the time the unlawful search occurred -- the Tenth Circuit stated:

The district court found that Officer Carvo knew that K.Y. was a minor, there was a large age difference between her and Mr. Christy, the two exchanged sexually explicit pictures, and that Mr. Christy traveled across state lines with K.Y. . . . Given those factual findings, it is a reasonable inference that a sexual relationship existed between Mr. Christy and K.Y. Officer Carvo also knew that K.Y. was potentially suicidal, had left her depression medication behind, and ran away from home with Mr. Christy. . . . Based on that knowledge, Officer Carvo’s belief that K.Y. was at risk for sexual victimization and assault was reasonable. Thus, Officer Carvo had reasonable grounds to believe that Mr. Christy engaged in sexual activity in violation of California law and coerced or enticed K.Y. to travel across state lines to engage in criminal sexual activity in violation of federal law. . . . The district court was correct in weighing this factor in favor of applying inevitable discovery.

United States v. Christy, 739 F.3d at 542. Analyzing the fourth factor -- evidence that the officers jumped the gun because they lacked confidence in their showing of probable cause and wanted to force the issue by creating a fait accompli -- the Tenth Circuit explained:

Mr. Christy argues that the deputies “jumped the gun” by forcing entry into his home due to their lack of confidence about probable cause. . . . Yet as the district court found, no evidence supports the theory that the deputies forced entry for that reason. . . . Instead, the deputies forced entry because they believed K.Y. was in danger. . . . Mr. Christy argues that the search was not in fact justified by exigent circumstances and points to the district court’s conclusion that it was not. . . . But that is beside the point. The record fully supports the reasonableness of the deputies’ assessment of danger. The district court was correct in weighing this factor in favor of the government.

United States v. Christy, 739 F.3d at 543. The Tenth Circuit concluded, therefore, that the Court properly applied the United States v. Souza factors. See 739 F.3d at 542.

### **ANALYSIS**

The Court will deny the Motion. The Court concludes that Loera may seek suppression of the child pornography evidence, because he admitted that the CDs and laptop on which the agents discovered child pornography were within his control and possession when the agents seized them. The Court holds that the First Warrant satisfies the Fourth Amendment’s particularity requirement, because it limits the agents’ search to evidence of computer fraud and electronic mail hijacking. The Court concludes that the agents’ on-site preview of Loera’s CDs during the execution of the First Warrant on November 20, 2012, was within the First Warrant’s scope, because the First Warrant authorized the agents to open image and video files, and files with last-modified and created dates before July 29, 2011. The Court further holds that, under Tenth Circuit law, with which the Court has concerns, the agents conducted an unlawful search when they continued searching Loera’s CDs for computer fraud and electronic mail hijacking after they discovered child pornography. The Court concludes, however, that the agents acted in good faith when they did so. The Court holds that Cravens was not permitted to open files on Loera’s CDs on November 27, 2012, for the limited purpose of providing a United States Magistrate Judge a description of four images depicting the sexual abuse of a child. The Court

concludes that, even if Cravens was not permitted to open the files on November 27, 2012, and even if those descriptions are excised from the Second Affidavit, probable cause to issue the Second Warrant still existed. The Court holds that, even if the Second Warrant, issued on November 29, 2012, suffered from an incurable defect, Nishida relied on that warrant in good faith when he searched Loera's CDs and laptop for child pornography. Finally, the Court holds that, even if the Second Warrant contained an incurable defect and Nishida did not execute the second warrant in good faith, the agents inevitably would have discovered child pornography. Accordingly, the Court will deny the Motion and will not suppress the child pornography.

**I. LOERA MAY SEEK SUPPRESSION OF THE CHILD PORNOGRAPHY.**

Loera may seek suppression of the child pornography. In its Response, the United States argues that Loera fails to establish the requisite standing to seek suppression of the child pornography, because he had not asserted a possessory interest in the evidence that he seeks to suppress. See Response at 6-7. In his Reply, Loera admits that the CDs and laptop on which the agents discovered child pornography were within his control and possession when the agents seized them. See Reply at 1. At the August 19, 2014, hearing, the United States conceded that, given Loera's admission in his Reply, he had sufficient standing to move to suppress the child pornography evidence. See Aug. 19, 2014 Tr. at 314:21-315:3 (Tuckman).

The Court notes that, in Minnesota v. Carter, the Supreme Court recognized that Rakas v. Illinois put an end to the Fourth Amendment standing analysis as separate from the substantive Fourth Amendment search analysis:

The Minnesota courts analyzed whether respondents had a legitimate expectation of privacy under the rubric of "standing" doctrine, an analysis that this Court expressly rejected 20 years ago in Rakas [v. Illinois] . . . . Central to our analysis [in Rakas v. Illinois] was the idea that in determining whether a defendant is able to show the violation of his (and not someone else's) Fourth Amendment rights, the "definition of those rights is more properly placed within the purview of

substantive Fourth Amendment law than within that of standing.”

Minnesota v. Carter, 525 U.S. at 87-88 (citations omitted). The Supreme Court has thus noted that the analysis under either approach -- the substantive Fourth Amendment doctrine that the rights that the Amendment secures are personal versus the separate notion of “standing” -- is the same and that Katz v. United States’ reasonable-expectation-of-privacy analysis has now been classified as a substantive Fourth Amendment test as opposed to a standing test. Rakas v. Illinois, 439 U.S. at 139.

Rigorous application of the principle that the rights secured by this Amendment are personal, in place of a notion of “standing,” will produce no additional situations in which evidence must be excluded. But we think the better analysis forthrightly focuses on the extent of a particular defendant’s rights under the Fourth Amendment, rather than on any theoretically separate, but invariably intertwined concept of standing.

Rakas v. Illinois, 439 U.S. at 139 (footnote omitted).

Given that the United States has conceded that Loera has sufficient standing to seek suppression of the child pornography evidence and that the agents’ opening of files on the media devices found at Loera’s residence constitute Fourth Amendment searches, the Court finds that Loera may seek to suppress the child pornography.

## **II. THE FIRST WARRANT SATISFIED THE FOURTH AMENDMENT’S PARTICULARITY REQUIREMENT.**

The Court concludes that the First Warrant was sufficiently particular. Loera contends that the First Warrant did not meet the Fourth Amendment’s particularity requirement, because it failed to “specify as nearly as possible the distinguishing characteristics of the goods to be seized.” Aug. 19, 2014 Tr. at 298:24-299:4 (Serna)(citing Cassady v. Goering). Loera asserts that “[t]he agents’ testimony that [the First Warrant] did not contain a restriction pertaining to time or dates of the files . . . supports invalidation of the warrant” for lack of particularity.

Supplement to Reply at 6-7. Moreover, Loera argues that the First Affidavit “contained no basis for probable cause to believe that evidence of wire fraud or unlawful interception of wire communications would be found in graphic image or video files.” Memorandum at 5 (citing United States v. Sells, 463 F.3d at 1157).

The United States responds that “the Tenth Circuit has ‘adopted a somewhat forgiving stance’” when faced with particularity challenges to warrants authorizing computer searches. Response at 6 n.4 (quoting United States v. Grimmer, 429 F.3d at 1270)(internal quotation marks omitted). The United States argues that, to satisfy particularity, a warrant seeking ESI must be “limited to a search for evidence of a violation of a particular federal statute.” Response at 6 n.4 (citing United States v. Christie, 717 F.3d at 1165). The Court agrees with the United States.

The Fourth Amendment mandates that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. The “manifest purpose” of the particularity requirement is “to prevent general searches.” Maryland v. Garrison, 480 U.S. at 84. “By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.” Maryland v. Garrison, 480 U.S. at 84.

The Tenth Circuit has emphasized that “practical accuracy rather than technical precision controls the determination of whether a search warrant adequately describes the place to be searched.” United States v. Burke, 633 F.3d 984, 992 (10th Cir. 2011)(citations omitted)(internal quotation marks omitted). A search warrant should “enable the searcher to

reasonably ascertain and identify the things authorized to be seized.” United States v. Wolfenbarger, 696 F.2d 750, 752 (10th Cir. 1982)(internal quotation marks omitted). A search warrant must contain “as much specificity as the government’s knowledge and circumstances allow.” United States v. Leary, 846 F.2d at 600. The Tenth Circuit has explained that, to satisfy the Fourth Amendment’s particularity requirement, a search warrant seeking ESI must “affirmatively limit the search to evidence of specific federal crimes or specific types of material.” United States v. Riccardi, 405 F.3d at 862 (citations omitted).

In United States v. Burgess, for example, the warrant authorized a search of “computer records,” and “items of personal property which would tend to show conspiracy to sell drugs, including pay-owe sheets, address books, rolodexes, pagers, firearms and monies.” 576 F.3d at 1091 (citations omitted)(internal quotation marks omitted). The Tenth Circuit held that the warrant “was not overly broad,” because it “contained sufficiently particularized language creating a nexus with the crime to be investigated -- drug trafficking.” 576 F.3d at 1091 (citations omitted)(internal quotation marks omitted). By contrast, in United States v. Riccardi, the warrant authorized the seizure of the defendant’s computer and “all electronic and magnetic media stored therein, together with all storage devises [sic] . . . and all electronic media stored within such devises [sic].” 405 F.3d at 852. The Tenth Circuit stated that the warrant “was not limited to any particular files, or to any particular federal crime.” 405 F.3d at 852. Consequently, the Tenth Circuit held: “By its terms, the warrant thus permitted the officers to search for anything -- from child pornography to tax returns to private correspondence,” making it “precisely the kind of ‘wide-ranging exploratory search that the Framers intended to prohibit.’” 405 F.3d at 863 (quoting Maryland v. Garrison, 480 U.S. at 84). See United States v. Brooks, 427 F.3d at 1252-53 (10th Cir. 2005)(finding warrant valid where it authorized a search of the

defendant's computer "for evidence of child pornography"); Davis v. Gracey, 111 F.3d 1472, 1479-80 (10th Cir. 1997)(finding warrant valid where it directed officers to seize equipment pertaining to the distribution or display of pornographic materials in violation of a specific state law).

The First Warrant was sufficiently particular. Similar to the warrant in United States v. Burgess, the First Warrant "was not overly broad," because it "contained sufficiently particularized language creating a nexus with the crime[s] to be investigated": computer fraud and electronic mail hijacking. 576 F.3d at 1091 (citations omitted)(internal quotation marks omitted). A reasonable interpretation of the First Warrant's language confined the items -- and the files within them -- to be seized and searched to those containing evidence of computer fraud and electronic mail hijacking. For example, paragraph 1 of Attachment B authorizes agents to seize "[a]ll records, in any form, relating to violations of Title 18 U.S.C. § 2511 (Interception and disclosure of wire, oral, or electronic communications prohibited) and Title 18 U.S.C. § 1030 (Fraud and related activity in connection with Computers)." Attachment B ¶ 1, at 2. Paragraph 2 permits agents to seize "[a]ny computers, cell phones, and/or electronic media that could have been used as a means to commit the offenses described in the warrant." Attachment B ¶ 2, at 2. Paragraph 4 authorizes agents to seize "[r]ecords and things evidencing the use of computers and/or the internet to commit the fraud activity described in the Search Warrant Affidavit . . . ." Attachment B ¶ 4, at 3. Moreover, paragraphs 1, 3, 4, and 6 of Attachment B set forth illustrative lists of the items to be seized. See Attachment B ¶¶ 1, 3, 4, 6, at 2-5; United States v. Riley, 906 F.2d 841, 844-45 (2d Cir. 1990)(holding that a warrant's description of items to be searched and seized is sufficiently particular if "delineated in part by an illustrative list").

Under the circumstances of the case, the agents had no information with which they



could have provided further clarity in the search warrant -- for example, by specifying the extensions, dates, or names of the files that they would need to search to uncover evidence of electronic mail hijacking and computer fraud. They had no idea what computer equipment or electronic devices that Loera would have used to access his electronic mail accounts, the hijacked electronic mail account, or the Domain, or where he could have concealed evidence that he had done so. Evidence of electronic mail hijacking and computer fraud could have been hidden on CDs, external hard drives, USB drives, cellular telephones, desktop or laptop computers, DVDs, or floppy disks. Usernames, passwords, electronic mail transmissions, or attachments to hijacked electronic mail transmissions could be saved in the form of electronic mail files (e.g., .msg, .dbx, .eml, and .mbox extensions), word processing files (e.g., .doc, .docx, .wpd, .rtf, .txt, and .wps extensions), spreadsheet files (e.g., .xls or .xlsx extensions), database files (e.g., accdb, .mdb, .ldb, and .wdb extensions), internet files (e.g., .html, .mhtml, .xml extensions), or image files (e.g., .jpg, .bmp, .gif, and .tiff extensions), to name just a few.<sup>11</sup>

Moreover, the agents had no way of knowing whether Loera had changed the extensions of incriminating files to conceal their real file types. As the United States Court of Appeals for the Ninth Circuit explained in United States v. Hill, 459 F.3d 966 (9th Cir. 2006): “Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.” 459 F.3d at 978. See United States v. Harding, 273 F. Supp. 2d 411, 424 (S.D.N.Y. 2003)(“Files containing graphical images may be assigned file extensions, including ‘TXT’, that typically are assigned to text files. Files containing text may be assigned file extensions, including ‘JPG’ or ‘GIF’, that typically are given to graphical image files.”). Especially in a case involving computer fraud and electronic

---

<sup>11</sup>See generally “List of File Formats,” Wikipedia, [http://en.wikipedia.org/wiki/List\\_of\\_file\\_formats](http://en.wikipedia.org/wiki/List_of_file_formats) (last visited Oct. 7, 2014).

hijacking -- crimes that require a certain level of technological sophistication to commit -- the agents had reason to suspect that Loera had both the ability and the inclination to conceal incriminating information on his technological devices in a variety of locations and formats.

The agents also had no way to know the names of the files in which Loera saved incriminating evidence -- making a prospective limitation on the names of files that could be searched impractical. As the United States Court of Appeals for the Third Circuit explained in United States v. Highbarger, 380 F. App'x 127 (3d Cir. 2010), “[s]uspects can easily hide information by mislabeling files, and, therefore, law enforcement officials are not required to accept a suspect’s designation of what is contained in a particular file.” 380 F. App'x at 130. The Ninth Circuit echoed this concern in United States v. Hill, stating: “Forcing police to limit their searches to files that the suspect has labeled in a particular way would be much like saying police may not seize a plastic bag containing a powdery white substance if it is labeled ‘flour’ or ‘talcum powder.’” 459 F.3d 966, 978 (citations omitted). See United States v. Williams, 592 F.3d 511, 522 (4th Cir. 2010)(“Surely, the owner of a computer, who is engaged in criminal conduct on that computer, will not label his files to indicate their criminality.”).

The agents also could not feasibly limit their search to a particular date range. Both Cravens and Nishida testified that the last-modified and created dates on files could be changed either intentionally or unintentionally. See May 20, 2014 Tr. at 64:4-24 (Cravens, Tuckman)(stating that he did not limit his search to files created after July, 2009, because he believed that the file dates could have been changed or inaccurate); May 20, 2014 Tr. at 164:8-11 (Nishida)(explaining that he did not limit his search to files created after July 2009, because the First Warrant did not contain a date restriction, and because he believed that “there could easily be evidence of the crime that doesn’t fit in that data range”). As an example, Cravens explained

that, if you manually change the date on your computer, “it would change all files created or modified after that, the dates would be different, and incorrect.” May 20, 2014 Tr. at 64:19-21 (Cravens). Nishida testified that there are a number of ways in which individuals can change the dates of files on CDs: “[S]ome software will allow you to burn the date, use the dates that were on the hard drives for the files, or use a date that the CD was burned, or you could pick an arbitrary date and just type it in while you’re burning . . . the CD.” May 20, 2014 Tr. at 219:19-24 (Nishida). Given the ease with which an individual may change the file dates on his or her computer, and the fact that this case concerned electronic mail hijacking and computer fraud -- crimes that inherently involve using technology to deceive others -- the First Warrant could not have imposed a date restriction without running the risk of losing a significant amount of relevant evidence.

Moreover, although the Tenth Circuit has not directly addressed the issue, multiple Tenth Circuit cases have found search warrants sufficiently particular despite not specifying a date range. See, e.g., United States v. Walser, 275 F.3d 981, 983-84 (10th Cir. 2001)(finding warrant sufficiently particular where it authorized officers to search for “[c]ontrolled substances, evidence of the possession of controlled substances, which may include, but not be limited to . . . records, and/or receipts, written or electronically stored, income tax records, checking and savings records.”); United States v. Burgess, 576 F.3d at 1083 (finding warrant sufficiently particular where it authorized officers to search the defendant’s “computer records” for “evidence to show the transportation and delivery of controlled substances.”). Consequently, the First Warrant did not lack sufficient particularity for failing to prescribe a limit the agents’ search to a particular date range.

The breadth of paragraph 3 of Attachment B similarly does not lead the Court to conclude that the First Warrant lacks sufficient particularity. Paragraph 3 states:

For any computers, cell phones, tablets, computer hard drives, or other physical objects upon which computer data can be recorded/stored (hereinafter, “COMPUTER”) that is called for by this warrant, or that might contain things otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- . . . .
- g. contextual information necessary to understand the evidence described in this attachment.

Attachment B ¶ 3, at 3. At first blush, these sections appear to allow the agents to search seemingly every file on every device discovered at Loera’s residence. Consequently, these provisions are similar to the warrant that the Tenth Circuit found invalid in United States v. Riccardi, which “permitted the officers to search for anything -- from child pornography to tax returns to private correspondence.” 405 F.3d at 863. There are, however, two significant differences between these passages and the warrant in United States v. Riccardi.

First, unlike the warrant in United States v. Riccardi, which was not limited to any federal crime, both the context of the First Warrant and the executing agents’ understanding of the scope of the First Warrant demonstrate that these sections were limited to evidence of computer fraud and electronic mail hijacking. Paragraph 3.a. restricts the agents’ search to “evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted.” Attachment B ¶ 3.a., at 3 (emphasis added). Paragraph 3.g. restricted the agents’ search to “contextual information necessary to understand the evidence

described in this attachment.” Attachment B ¶ 3.g., at 3 (emphasis added). When read with the rest of Attachment B, it is evident that these sections were limited to evidence of computer fraud and electronic mail hijacking. See, e.g., Attachment B ¶ 1, at 2 (stating “[a]ll records, in any form, relating to violations of Title 18 U.S.C. § 2511 . . . and Title 18 U.S.C. § 1030 . . . .”); Attachment B ¶ 2, at 3 (stating “[a]ny computers that could have been used as a means to commit the offenses described on the warrant . . . .”); Attachment B ¶ 4, at 3 (stating “[r]ecords and things evidencing the use of computers and/or the intent to commit the fraud activity described in the Search Warrant Affidavit”). The executing agents’ testimony at the suppression hearing -- that the First Warrant authorized them only to find and seize evidence of computer fraud and electronic mail hijacking -- also reinforces this interpretation. See May 20, 2014 Tr. at 53:7-11 (Cravens, Tuckman); id. at 152:6-8 (Nishida, Tuckman); id. at 160:5-11 (Nishida, Tuckman).

Second, unlike the warrant in United States v. Riccardi, which “did not describe the objects of the search with as much specificity as the government’s knowledge and circumstances allow[ed],” 405 F.3d at 863, the agents in this case did not have any information with which they could have provided further clarity in paragraphs 3.a. or 3.g. Evidence of who “used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted” was essential to establishing who perpetrated the computer fraud and electronic mail hijacking. Attachment B ¶ 3a., at 3. Unless Loera confessed that he possessed these items, this evidence was the only way for the United States to establish who committed the computer fraud and electronic mail hijacking. The Tenth Circuit has upheld similar sections of warrants that authorize law enforcement to seize “indicia of occupancy” from a suspect’s home -- e.g., telephone bills, letters, electronic mail transmissions. In United States v. Walser, for example, the Tenth Circuit upheld a warrant containing a similar clause that authorized officers to search

for and seize, among other things, “records that show or tend to show ownership or control of the premises and other property used to facilitate the distribution and delivery [of] controlled substances.” 275 F.3d at 984.

Other United States Courts of Appeals have upheld similar sections of search warrants that seek “indicia of occupancy.” In United States v. Blakeney, 942 F.2d 1001 (6th Cir. 1991), for example, the warrant authorized officers to seize “[i]ndicia of occupancy, residency, and/or ownership of premises, including but not limited to, utility and telephone bills, cancelled envelopes, deeds, leases, personal telephone books, and safe deposit box keys.” 942 F.2d at 1026. In that case, the United States Court of Appeals for the Sixth Circuit found that the “indicia of occupancy” clause satisfied the Fourth Amendment, because it tended to prove facts that would be relevant in establishing the identity of the perpetrators of the offense. 942 F.2d at 1027.

Regarding paragraph 3.g., the agents did not possess any additional information that would have allowed them to further specify the contextual information that would assist them in understanding the evidence seized. Because the agents did not know what devices they would encounter, in what file formats they would find this information, when this information was created or last-modified, or where it would be saved, the First Warrant was made “with as much specificity as the government’s knowledge and circumstances allow[ed],” United States v. Leary, 846 F.2d at 600. The Court, accordingly, holds that the First Warrant satisfies the Fourth Amendment’s particularity requirement.

**III. THE AGENTS’ ON-SITE PREVIEW OF LOERA’S CDS DURING THE EXECUTION OF THE FIRST WARRANT ON NOVEMBER 20, 2012, WAS WITHIN THE FIRST WARRANT’S SCOPE.**

The Court concludes that the agents’ preliminary preview of Loera’s CDs during the

execution of the First Warrant was within the First Warrant's scope. The Court holds that the First Warrant authorized the agents to open image and video files. Moreover, the Court concludes that the First Warrant authorized the agents to open files dated before July 29, 2011.

**A. THE FIRST WARRANT AUTHORIZED THE AGENTS TO OPEN IMAGE AND VIDEO FILES.**

The Court holds that the First Warrant authorized Cravens and Nishida to open image and video files. Loera contends that the First Warrant limited the scope of the November 20, 2012, search to "evidence pertaining to . . . unlawful interception of wire communications and fraud in relation to computers." Memorandum at 4. Loera points out that the First Affidavit did not allege that Estrada intercepted images or videos through the electronic mail accounts at the Domain. See Supplement to Reply at 7. Loera contends that, accordingly, Nishida and Cravens went beyond the scope of the First Warrant when they opened image and video files on Loera's CDs. See Supplement to Reply at 7. In Loera's view, the agents should have used software to restrict their searches to text files. See Aug. 19, 2014 Tr. at 287:23-288:4 (Serna); id. at 290:12-292:14 (Serna).

In response, the United States points out that the First Warrant "authorized agents to search and seize, among other things, pictures that could be found on 'physical objects upon which computer data can be recorded/stored,' such as the CDs at issue here." Response at 7 (quoting Attachment B ¶¶ 3, 3a., at 3)). The United States also argues that the First Warrant authorized the agents to open files that appeared to be images and videos, because file names and extensions can be changed to conceal evidence. See Response at 7 n.5. To support this contention, the United States quotes from United States v. Burgess, in which the Tenth Circuit stated:

It is unrealistic to expect a warrant to prospectively restrict the scope of a search

by directory, filename, or extension or to attempt to structure search methods -- that process must remain dynamic . . . . [I]llegal activity may not be advertised even in the privacy of one's personal computer -- it could be well coded or otherwise disguised.

Response at 7 n.5 (quoting United States v. Burgess, 576 F.3d at 1093-94)(brackets added)(internal quotation marks omitted)). The United States also argues that the law did not require the agents to seize everything from Loera's residence and analyze it at the FBI laboratory with search-limiting software. See Aug. 19, 2014 Tr. at 315:12-318:13 (Tuckman). The Court agrees with the United States.

The Tenth Circuit has held that a computer search "may be as extensive as reasonably required to locate the items described in the warrant." United States v. Grimmer, 439 F.3d at 1270 (citations omitted)(internal quotation marks omitted). Multiple sections of Attachment B authorize the agents to open image files on Loera's CDs. Paragraph 3.a. explicitly authorizes them to search for "photographs." Attachment B ¶ 3a., at 3. Paragraph 1 permits the agents to seize "[a]ll records, in any form, relating to" computer fraud and electronic mail hijacking. Attachment B ¶ 1, at 2 (emphasis added). Paragraph 1, therefore, authorizes Nishida and Cravens to open image files to determine if they contain evidence of computer fraud and electronic mail hijacking -- e.g., logs of instant messaging conversations between Loera and Estrada, screenshots of hijacked electronic mail transmissions, digital photographs of the subscriber information for the Tacori GoDaddy account, or digital photographs of the Domain's username and password. See May 20, 2014 Tr. at 62:21-22 (Cravens, Tuckman)(explaining that he opened image files, in part, because they "could have been a screen shot of e-mail or domain hijacking"). Finally, paragraph 6 authorized agents to seize: "Any and all documents, printouts, hand written statements, electronic communications, and in whatever form related to the following: a. The Susana2010.com domain; b. Communications with GoDaddy.com and



DomainsByProxy.com; c. The SusanaPAC.com domain; [and] d. The interception of emails related to the Susana2010.com Domain.” Attachment B ¶ 6, at 4 (emphasis added). Thus, pursuant to paragraph 6, the agents can open the image files on Loera’s CDs to determine if they contained screenshots of documents or electronic communications relating to the Domain, GoDaddy, or intercepted electronic mail transmissions.

Paragraph 3.a. also authorizes the agents to open video files. A reasonable interpretation of “evidence of who used, owned, or controlled the [seized items] at the time the things described in this warrant were created, edited, or deleted” includes video files, because those files could contain videos made by and/or of the individuals who used, owned, or controlled the media seized from Loera’s residence during the relevant period. Attachment B ¶ 6, at 3. Moreover, even if the First Warrant did not specifically authorize the agents to open image or video files, the reasons that the Court articulated previously for not requiring the First Warrant to prescribe a particular search methodology apply with equal force here. First, Loera could have converted electronic mail transmissions, bills for the Domain, or other text documents related to computer fraud and electronic mail hijacking into images. Second, Loera could have -- either intentionally or unintentionally -- changed the extensions of text files containing evidence of computer fraud and electronic mail hijacking so that they appeared to be image or video files. See May 20, 2014 Tr. at 62:24-63:8 (Cravens, Tuckman)(explaining that he opened image files, in part, because “[t]he extension could have been different than what it actually was. . . . [I]f you double click and get the box, you can change . . . the file extension right there”).

Loera’s argument that the agents should have seized all of the items from Loera’s residence to analyze them at an FBI laboratory using search-limiting software similarly lacks a sound basis in the law. Loera conceded as much when he stated that his “argument is not that

there is some constitutional requirement that . . . the law enforcement take everything back to the lab,” but instead that it would have been practical for them to do so. Aug. 19, 2014 Tr. at 323:22-25 (Serna). The law does not require law enforcement to use the least restrictive means or search-limiting software to execute a search warrant. Cf. United States v. Brooks, 427 F.3d at 1251 (“The Tenth Circuit has never required warrants to contain a particularized computer search strategy.”). Instead, a search “may be as extensive as reasonably required to locate the items described in the warrant.” United States v. Grimmett, 439 F.3d at 1270 (citations omitted)(internal quotation marks omitted). Moreover, given that the First Warrant authorized the agents to open image files, the agents likely would have discovered child pornography on Loera’s CDs even if they had used search-limiting software. The Court, accordingly, concludes that the agents did not exceed the First Warrant’s scope when they opened image and video files on Loera’s CDs on November 20, 2012.

**B. THE FIRST WARRANT AUTHORIZES THE AGENTS TO OPEN FILES WITH LAST-MODIFIED DATES BEFORE JULY 29, 2011.**

The Court concludes that the First Warrant authorizes Cravens and Nishida to open files with last-modified dates before July 29, 2011. Loera argues that there are three problems with the agents’ decision to disregard the file dates in searching Loera’s CDs. See Supplement to Reply at 4. First, Loera contends that disregarding the file dates turned the First Warrant into a “general exploratory warrant” that the Tenth Circuit and the Supreme Court have found unconstitutional. Supplement to Reply at 4. Second, Loera argues that, contrary to the United States’ assertion that the First Warrant does not put any restriction on time or dates, the First Affidavit seeks only electronic mail transmissions sent “during the period of time the Domain is believed to have been compromised by [Loera and Estrada]” -- which began on July 29, 2011. Supplement to Reply at 5 (emphasis in Supplement to Reply but not source)(quoting First

Affidavit at 8). Loera asserts that, “[c]onsequently, regardless of what method, manner or mode used by government agents to view or search Mr. Loera’s storage media or computer, the November 19 search warrant could not and did not authorize opening any files dated in 2009, or otherwise from prior to July 29, 2011.” Supplement to Reply at 5.

Third, Loera challenges the United States’ contention that the agents could disregard the file dates, because they could have been changed. See Supplement to Reply at 6. Loera argues that there was “not a single indication” in the First Warrant that the dates of the files on Loera’s CDs were changed. Supplement to Reply at 6. Loera also highlights that Nishida testified that there was no evidence that the file dates on Loera’s CDs had been changed. See Supplement to Reply at 6 (citations omitted). Loera explained that he was not arguing that the file dates on Loera’s laptop and CDs are “off somewhat.” Aug. 19, 2014 Tr. at 297:18-19 (Serna). Instead, Loera asserted that there is a two-to-three year difference between the alleged electronic mail hijacking and computer fraud on which the First Warrant focuses -- which began in 2011 -- and the files that Cravens and Nishida opened -- which contain last-modified dates from 2008 and 2009. See Aug. 19, 2014 Tr. at 297:19-298:2 (Serna). In Loera’s view, given this difference, the First Warrant does not permit Cravens and Nishida to open these files.

Loera’s arguments have no sound basis in law or fact. Multiple sections of the First Warrant explicitly authorize the agents to open files on Loera’s media without specifying a date range. For example, Paragraph 1 of Attachment B does not contain a date restriction: “[a]ll records, in any form, relating to violations of Title U.S.C. § 2511 (Interception and disclosure of wire, oral, or electronic communications prohibited) and Title 18 U.S.C. § 1030 (Fraud and related activity in connection with Computers), involving Jason Loera and others.” Attachment B ¶ 1, at 2. Multiple subsections of Paragraph 1 -- which provide examples of the information

the agents may seize under Paragraph 1 -- do not specify a date range:

- a. Usernames, passwords, and other account information for email accounts, Google Apps accounts, domain accounts, accounts for credit, debit, or gift cards, and online storage accounts;
- b. Records which are related to the use of computer programs to re-direct email from one domain to another;
- . . . .
- e. Records relating to the provision of internet and phone service;
- f. Records showing the technical or computer knowledge.

Attachment B ¶¶ 1.a., b., e., f., at 2. Paragraph 3 of Attachment B does not contain a date restriction: “For any computers, cell phones, tablets, computer hard drives, or other physical objects upon which computer data can be recorded/stored (hereinafter, “COMPUTER”) that is called for by this warrant, or might contain things otherwise called for by this warrant.”

Attachment B ¶ 3, at 3. Neither do the subsections of Paragraph 3. See, e.g., Attachment B ¶ 3.d., at 3 (“[E]vidence of the times the COMPUTER was used . . . .”); Attachment B ¶ 3.g., at 3 (“[C]ontextual information necessary to understand the evidence described in this attachment . . . .”). Paragraph 7 of Attachment B does not contain a date restriction: “Any and all records in whatever form related to email accounts maintained, controlled or used in any manner by Jason Loera.” Attachment B ¶ 7, at 5. To be sure, a few sections in Attachment B specify a date range for the information sought. For example, paragraph 5 authorizes the agents to search for and seize “[a]ny and all statements for bank accounts, which include transactions from June 1, 2011 to the present.” Attachment B ¶ 5, at 4. Paragraph 1.d. similarly allows the agents to search for and seize “[a]ll bank records, checks, credit or debit card bills, account information, and other financial records from June 2011 to the present.” Attachment B ¶ 1.d., at 2. Rather than demonstrating that the First Warrant restricts the agents’ search to files created or

last modified after July 29, 2011, however, that the First Warrant only includes date restrictions in these particular sections demonstrates that the rest of the First Warrant is meant to be unrestricted. Consequently, the agents did not exceed the scope of the First Warrant by opening files dated before July 29, 2011.

**IV. UNDER TENTH CIRCUIT LAW, WITH WHICH THE COURT RESPECTFULLY HAS SOME CONCERNS, THE AGENTS CONDUCTED AN UNLAWFUL SEARCH WHEN THEY CONTINUED SEARCHING LOERA'S CDS FOR COMPUTER FRAUD AND ELECTRONIC MAIL HIJACKING AFTER THEY DISCOVERED CHILD PORNOGRAPHY.**

Under Tenth Circuit law, with which the Court respectfully has concerns, the agents conducted an unlawful search when they continued opening files on Loera's CDs after discovering child pornography. Loera contends that the First Warrant did not authorize Cravens and Nishida to continue previewing the CDs after Cravens discovered child pornography. See Memorandum at 8-9 (citing United States v. Carey, 172 F.3d at 1273). By doing so, Loera argues, Nishida and Cravens "transformed the search warrant for evidence of . . . wire fraud pertaining to Governor Martinez's e-mails into a 'general warrant' and resulted in a general and illegal search of the four CDs." Memorandum at 7.

In response, the United States attempts to distinguish this case from United States v. Carey. The United States explains that, in United States v. Carey, after discovering child pornography, the searching officer abandoned his warrant-authorized search for drug-related evidence "to look for more child pornography" -- and did not resume his original search for five hours. Response at 9 (quoting United States v. Carey, 172 F.3d at 1273)(internal quotation marks omitted). The United States argues that, unlike the officer in United States v. Carey, Nishida and Cravens did not abandon their warrant-authorized search after finding evidence of child pornography, but instead continued to search for evidence of electronic mail hijacking and

computer fraud. See Response at 9 (citations omitted). The United States contends that this difference is significant, because Judge Baldock stated in his United States v. Carey concurrence that, “if the record showed that Detective Lewis had merely continued his [warrant-authorized] search for drug-related evidence, and, in doing so, continued to come across evidence of child pornography, I think a different result would be required.” Response at 9 (alterations in Response but not in Judge Baldock’s opinion)(quoting United States v. Carey, 172 F.3d at 1277)(Baldock, J., concurring)). The Court reluctantly agrees with Loera.

The Tenth Circuit has not been clear in indicating what law enforcement officers must do if, while executing a search warrant for ESI, they discover evidence of crimes not sought by the search warrant. In United States v. Carey, a detective obtained a warrant that authorized him to search the defendant’s computer for “names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances.” 172 F.3d at 1271. While searching the computer, the detective found what he described as a “JPG file” that contained child pornography. 172 F.3d at 1271. The detective then downloaded approximately two hundred forty-four JPG files onto nineteen floppy disks. See 172 F.3d at 1271. The detective looked at “about five to seven” files on each disk -- a process that took approximately five hours -- before continuing his search for evidence of drug transactions. 172 F.3d at 1271.

At the suppression hearing, the detective testified that, “although the discovery of the [first child pornography image] was completely inadvertent, when he saw [that image], he developed probable cause to believe the same kind of material was present on the other image files.” 172 F.3d at 1271. The detective later backtracked, stating that he “wasn’t conducting a search for child pornography” when he continued to open the image files, but that it was simply

“what those [files] turned out to be.” 172 F.3d at 1271 (internal quotation marks omitted). Based on the detective’s testimony, the Tenth Circuit, in an opinion that Judge Porfilio authored, and Judges McWilliams and Baldock joined, found that the child pornography was not “inadvertently discovered,” because the detective temporarily abandoned his warrant-authorized search to look for child pornography. 172 F.3d at 1273. The Tenth Circuit explained that,

the case turns upon the fact that each of the files containing pornographic material was labeled “JPG” and most featured a sexually suggestive title. Certainly after opening the first file and seeing an image of child pornography, the searching officer was aware -- in advance of opening the remaining files -- what the label meant. When he opened the subsequent files, he knew he was not going to find items related to drug activity as specified in the warrant.

172 F.3d at 1274. The Tenth Circuit concluded, accordingly, that the detective “exceeded the scope of the warrant in this case.” 172 F.3d at 1276.

The Tenth Circuit was careful to state, however, that the result in the case was “predicated only upon the particular facts of this case, and a search of computer files based on different facts might produce a different result.” 127 F.3d at 1276 (footnote omitted). Moreover, Judge Baldock stated, in his concurring opinion, that, “if the record showed that [the detective] had merely continued his search for drug-related evidence and, in doing so, continued to come across evidence of child pornography, . . . a different result would be required.” 172 F.3d at 1277 (Baldock, J., concurring).

After United States v. Carey, however, the Tenth Circuit faced a similar issue in United States v. Walser in 2001. In United States v. Walser, police officers obtained a warrant to search a defendant’s hotel room for “[c]ontrolled substances, evidence of the possession of controlled substances, which may include, but not be limited to . . . records, and/or receipts, written or electronically stored, income tax records, checking and savings records, records that show or tend to show ownership or control of the premises.” 275 F.3d at 983-84 (citations omitted).

While executing the search warrant, the officers discovered a laptop computer. See 275 F.3d at 984. Believing that the laptop could contain ledgers of drug transactions or images of drug use, the officer decided to search the laptop's hard drive. See 275 F.3d at 984. During the search, the officer discovered child pornography. See 275 F.3d at 984-85. The officer immediately stopped his search and did not resume it until after he had obtained a warrant for child pornography. See 275 F.3d at 985. In an opinion that Judge Seymour authored, and Judges Holloway and Van Bebber joined, the Tenth Circuit upheld the search. See 275 F.3d at 986-87. The Tenth Circuit explained that, when an officer "come[s] across relevant computer files intermingled with irrelevant computer files" while executing a search warrant, the officers "'may seal or hold' the computer pending 'approval by a magistrate of the conditions and limitations on a further search' of the computer." 275 F.3d at 986 (quoting United States v. Carey, 172 F.3d at 1275). The Tenth Circuit explained that, had the officer "conducted a more extensive search than he did here by rummaging in folders and files beyond those he searched, he might well have exceeded the bounds of the warrant and the requirements of Carey." 275 F.3d at 987. The Tenth Circuit concluded, however, that "no such wholesale searching occurred here," because the officer "showed restraint by returning to the magistrate for a new warrant before commencing a new search for evidence of child pornography." 275 F.3d at 987

In 2009, the Tenth Circuit decided United States v. Burgess. In United States v. Burgess, police officers obtained a warrant to search the defendant's "computer records" for "evidence to show the transportation and delivery of controlled substances." 576 F.3d at 1083. While executing the search warrant, officers discovered two external hard drives and a laptop. See 576 F.3d at 1083. An officer began previewing images on one of the external hard drives for "trophy photos" -- i.e., "pictures of a person holding [a] controlled substance in front of a stack of



money.” 576 F.3d at 1084 (citations omitted)(internal quotation marks omitted). The officer viewed the images in a “gallery view,” in which multiple small photographs are displayed on a single page. 576 F.3d at 1084. After viewing 200-300 images, the officer discovered child pornography. See 576 F.3d at 1084. The officer immediately closed the previewing program and did not resume his search until he obtained a search warrant for child pornography. See 576 F.3d at 1084. In an opinion that Judge O’Brien authored, and Judges Tacha and McConnell joined, the Tenth Circuit found the officer’s actions reasonable, stating: “[A]s our cases seem to require, [the officer] immediately closed the gallery view when he observed a possible criminal violation outside the scope of the warrant’s search authorization and did not renew the search until he obtained a new warrant.” 576 F.3d at 1094-95 (footnotes omitted).

As in United States v. Carey, United States v. Walser, and United States v. Burgess, Nishida and Cravens inadvertently discovered child pornography while searching for evidence of another crime. See May 20, 2014 Tr. at 60:5-7 (Cravens); id. at 158: 20-22 (Nishida, Tuckman). Unlike the officers United States v. Walser and United States v. Burgess, however, Cravens and Nishida did not immediately stop their searches upon discovering child pornography. See May 20, 2014 Tr. at 65:10-17 (Cravens, Tuckman); id. at 116:3-12 (Cravens, Serna); id. at 161:17-162:18 (Nishida, Tuckman). After discovering child pornography on one of Loera’s CDs, Cravens ejected that CD and continued opening files on Loera’s other CDs to determine if they contained evidence of computer fraud and electronic mail hijacking. See May 20, 2014 Tr. at 61:12-13 (Cravens); id. at 65:10-17 (Cravens, Tuckman). Cravens later discovered another child pornography image on another of Loera’s CDs. See May 20, 2014 Tr. at 67:18-68:4 (Cravens, Tuckman). Nishida also found child pornography on one of Loera’s CDs. See May 20, 2014 Tr. at 161:17-162:18 (Nishida, Tuckman). After finding child pornography on one of

Loera's CDs, Nishida opened two or three more files on that CD to determine if they contained evidence of computer fraud or electronic mail hijacking. See May 20, 2014 Tr. at 161:17-162:18 (Nishida, Tuckman). The agents' searches were, therefore, closer to that of the detective in United States v. Carey, who, after discovering child pornography on one floppy disc, continued to open five to seven image files on each of nineteen floppy discs, than the searches that the Tenth Circuit found permissible in United States v. Burgess and United States v. Walser.

Unlike in United States v. Carey, however, where all of the files that the detective opened after discovering the first child pornography image were clearly labeled as image files and "most featured a sexually suggestive title," 172 F.3d at 1274, there is no evidence indicating whether any of the files in which the agents here discovered child pornography were clearly labeled as image files or whether they featured sexually suggestive titles. Moreover, unlike the detective in United States v. Carey, who testified that he believed he had probable cause to search the other floppy discs for child pornography after discovering the first child pornography image, the agents testified that, after discovering child pornography, they continued to search Loera's CDs for evidence of electronic mail hijacking and computer fraud. See United States v. Carey, 172 F.3d at 1271; May 20, 2014 Tr. at 65:15-17 (Cravens, Tuckman); id. at 165:4-17 (Nishida, Tuckman).

This case, thus, presents the scenario that Judge Baldock envisioned in his concurring opinion in United States v. Carey, in which he stated that, "if the record showed that [the detective] had merely continued his search for drug-related evidence and, in doing so, continued to come across evidence of child pornography, . . . a different result would be required." 172 F.3d at 1277 (Baldock, J., concurring). The majority opinion in United States v. Carey, and the Tenth Circuit's later decision in United States v. Burgess, however, seem to require officers to

immediately stop their warrant-authorized searches upon discovering evidence of another crime.

The majority opinion in United States v. Carey states:

[L]aw enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in the warrant. Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents.

172 F.3d at 1275. In United States v. Burgess, the Tenth Circuit said, in dicta, that, “as our cases seem to require, [the officer] immediately closed the gallery view when he observed a possible criminal violation outside the scope of the warrant’s search authorization and did not renew the search until he obtained a new warrant.” 576 F.3d at 1094-95 (emphasis added)(footnotes omitted). “While the Court may not be bound by Tenth Circuit dicta, the Court takes seriously anything that the Tenth Circuit says.” United States v. Ganadonegro, 854 F. Supp. 2d 1088, 1124 (D.N.M. 2012)(Browning, J.). The Court concludes that the Tenth Circuit’s statements in United States v. Burgess and United States v. Walser more accurately reflect Tenth Circuit law on this issue than Judge Baldock’s concurrence in United States v. Carey. Given that Nishida and Cravens did not immediately stop searching Loera’s CDs upon discovering child pornography, as Tenth Circuit law “seem[s] to require,” United States v. Burgess, 576 F.3d at 1094-1095, the Court concludes that the agents conducted an unlawful search under Tenth Circuit precedent when they continued their warrant-authorized searches.

Despite its holding, the Court questions whether the Tenth Circuit intended to announce a bright-line rule that would require every officer who discovers evidence of another crime, while executing a computer search warrant, to immediately cease his or her warrant-authorized search, and obtain another warrant. The Court has three concerns about such a rule.

First, a rule requiring officers to immediately stop their warrant-authorized computer

searches upon discovering evidence of another crime conflicts with the Supreme Court's holding in Horton v. California. In that case, an officer obtained a warrant to search the defendant's house for the proceeds of a robbery. See 496 U.S. at 131. While executing the search warrant, the officer found, and subsequently seized, among other things, a machine gun, a .38-caliber revolver, two "stun guns," and a handcuff key. 496 U.S. at 131. The officer did not find, however, any evidence that the search warrant sought. See 496 U.S. at 131. The officer testified that, while executing the search warrant, he was also looking for evidence outside the search warrant's scope. See 496 U.S. at 131. Finding the officer's subjective intentions during the search irrelevant, the Supreme Court explained, in an opinion that the Honorable Justice John P. Stevens, Associate Justice of the Supreme Court, wrote, and Chief Justice Rehnquist, Justices White, Blackmun, O'Connor, Scalia, and Kennedy joined:

[E]venhanded law enforcement is best achieved by the application of objective standards of conduct, rather than standards that depend upon the subjective state of mind of the officer. The fact that an officer is interested in an item of evidence and fully expects to find it in the course of a search should not invalidate its seizure if the search is confined in area and duration by the terms of a warrant.

496 U.S. at 138. Because the items seized "were discovered during a lawful search authorized by a valid warrant," and their seizure was justified by the plain-view exception, the Supreme Court found the officer's search constitutional. 496 U.S. at 142. In justifying its holding, the Supreme Court stated that a hypothetical presented in the concurring and dissenting opinion of the Honorable Byron R. White, Associate Justice of the Supreme Court, in Coolidge v. New Hampshire, 403 U.S. 443 (1971)(White, J., concurring and dissenting), is "instructive":

Let us suppose officers secure a warrant to search a house for a rifle. While staying well within the range of a rifle search, they discover two photographs of the murder victim, both in plain sight in the bedroom. Assume also that the discovery of the one photograph was inadvertent but finding the other was anticipated. . . . [I]n terms of the "minor" peril to Fourth Amendment values there is surely no difference between these two photographs: the interference with

possession is the same in each case and the officers' appraisal of the photograph they expected to see is no less reliable than their judgment about the other. And in both situations the actual inconvenience and danger to evidence remain identical if the officers must depart and secure a warrant." Id. at 516.

Horton v. California, 496 U.S. at 139 (quoting Coolidge v. New Hampshire, 403 U.S. at 516 (White, J., concurring and dissenting)). Although the Supreme Court did not explain whether the officer discovered the guns and other incriminating items simultaneously, or at different points while executing the search warrant, its holding is clear: so long as an officer acts within the scope of the search warrant -- i.e., searches only items that may reasonably contain the evidence that the warrant seeks -- it is irrelevant whether the officer either intends to find or inadvertently discovers evidence outside of the warrant's scope. See Horton v. California, 496 U.S. at 142. Although Horton v. California did not address computer searches, the Court finds it difficult to conclude that the privacy interests implicated by computer searches are so substantial -- and so distinct from every other search context -- that longstanding Supreme Court jurisprudence does not apply.

Second, the Court finds it difficult to conclude that such a rule would provide any greater Fourth Amendment protections. To conduct a computer search, officers have to satisfy a number of requirements. Before the search, they must provide a neutral Magistrate Judge with sufficient probable cause to believe that the places they intend to search contain evidence of a crime. They must also explain with sufficient particularity the evidence for which they are searching and the items they must search to find it. During the search, the officer cannot act outside the search warrant's scope -- i.e., he or she can search only items that may reasonably contain the objects of his warrant-authorized search. For a few hundred years, society has concluded that these requirements provide sufficient protection from unwarranted invasions of privacy by law enforcement.

The Tenth Circuit rule adds an additional, unprecedented, step that would require officers -- who have already obtained a warrant and are acting within its scope -- to stop what they are doing and obtain a second warrant when they find evidence of another crime. Under this rule, there would be no Fourth Amendment violation where an officer conducts a warrant-authorized computer search, confines his or her search to the scope of the warrant, and finds no evidence of a crime. There similarly would be no Fourth Amendment violation where an officer conducts a warrant-authorized computer search, confines his or her search to the scope of the warrant, and finds only evidence of the crime for which he or she is searching. By contrast, there would be a Fourth Amendment violation where the officer conducts a warrant-authorized computer search, confines his or her search to the scope of the warrant, finds evidence of another crime, and continues searching within the scope of the warrant. There would be a violation despite the officer not viewing any additional information beyond what the search warrant authorizes. Rather than protecting privacy rights, the only discernible impact of this rule would be to make the execution of computer search warrants less efficient.<sup>12</sup>

---

<sup>12</sup>The Court recognizes that the Supreme Court unanimously held in Riley v. California, 134 S. Ct. 2473 (2014), in an opinion that Chief Justice Roberts authored, that officers must obtain a warrant to search a cellular telephone seized during a lawful arrest. See 132 S. Ct. at 2495 (“Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple -- get a warrant.”). The Court has no disagreement with such a requirement. In fact, the Court reached the same conclusion more than ten years before the Supreme Court’s decision in Riley v. California. See United States v. Morales-Ortiz, 376 F. Supp. 2d 1131, 1139 (D.N.M. 2004)(Browning, J.) (“An individual has an expectation of privacy in an electronic repository for personal data, including cell telephones and pager data.”).

The Court’s concern with the Tenth Circuit’s rule is that it grants greater procedural protections to an individual’s cellular telephone, computer, and other devices in which he or she can store electronic information than those afforded to an individual’s home. Under the Tenth Circuit’s rule, while an officer searching a home pursuant to a search warrant can continue his warrant-authorized search upon discovering evidence of another crime, he or she cannot do so while executing a computer search warrant. Such a rule is at odds with the Supreme Court’s longstanding position that, when it comes to Fourth Amendment protections, of the four items that the Fourth Amendment lists -- “persons, houses, papers, and effects,” U.S. Const. amend. IV

Second, the Tenth Circuit is an outlier in imposing such a rule. The United States Court of Appeals to confront this issue have unanimously approved of officers continuing their warrant-authorized computer searches upon discovering evidence of another crime. Specifically, the United States Courts of Appeals for the Third, Fourth, Seventh, Ninth, and Eleventh Circuits have all done so. See United States v. Stabile, 633 F.3d 219, 240 (3d Cir. 2011)(Van Antwerpen, J., joined by Jordan, & Hardiman, JJ.)(upholding denial of motion to suppress where officers continued warrant-authorized search of the defendant's computer for financial crimes after discovering child pornography); United States v. Williams, 592 F.3d 511, 521-24 (4th Cir. 2010)(Niemeyer, J., joined by Duncan, & Jones, JJ.)(upholding search where the officer continued his warrant-authorized search of the defendant's computer for evidence of "making threats and computer harassment" after discovering child pornography); United States v. Miranda, 325 F. App'x 858, 859-60 (11th Cir. 2009)(per curiam)(Tjoflat, joined by Dubina, & Black, JJ.)(upholding search where officer continued his warrant-authorized search for evidence of counterfeit software after discovering child pornography); United States v. Wong, 334 F.3d

---

-- the home is "first among equals." Florida v. Jardines, 133 S. Ct. at 1414. See Kyllo v. United States, 533 U.S. 27, 31 (2001)("[T]he right of a man to retreat into his own home and there be free from unreasonable governmental intrusion" is "at the very core" of the Fourth Amendment). To be sure, the Supreme Court stated in Riley v. California that,

it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." United States v. Kirschenblatt, 16 F.2d 202, 203 (C.A.2). If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form -- unless the phone is.

134 S. Ct. at 2490-91 (emphasis in original). Although this passage may indicate the Supreme Court's willingness to provide greater Fourth Amendment protections in the ESI context in the future, the Court finds it difficult to conclude that such increased protections are either necessary or required under current Supreme Court precedent.

831, 835 (9th Cir. 2003)(Brunetti, J., joined by Tashima, & Ezra, JJ.)(upholding denial of motion to suppress where the officer continued his warrant authorized search of the defendant's computer for, among other things, "[a]ny maps, receipts, or writings, depicting Churchill County Nevada" after discovering child pornography).

United States v. Giberson, 527 F.3d 882 (9th Cir. 2008), is a typical case. In United States v. Giberson, an agent obtained a warrant to search the defendant's residence for:

(1) records or documents that appear to show ownership of assets or property; (2) records or documents from financial institutions in [the defendant's] name or the names of any known or unknown aliases; (3) records and correspondence relating to identification cards; (4) records, documents or correspondence . . . related to the use or attempted use of other individual's identities; (5) correspondence, records and documents relating to [the defendant's] or his aliases' earnings and employment; (6) tax records; (7) documents or records showing receipt of income or expenditure of funds; and (8) records referring to [the defendant's] employer.

527 F.3d at 885 (internal quotation marks omitted). While executing the search warrant, the agent discovered child pornography on the defendant's computer. See 527 F.3d at 885. The agent continued his warrant-authorized search and, "as he came across images of child pornography, he printed out a sampling." 527 F.3d at 885. The agent later obtained a warrant to search the defendant's computer for child pornography. See 527 F.3d at 885. In an opinion that Judge Wallace authored, and Judges Schroeder and Benitez joined, the Ninth Circuit found the agent's continued search of the defendant's computer reasonable. See 527 at 890-91. The Ninth Circuit also explained that its holding was "not inconsistent with United States v. Carey." 527 F.3d at 890. The Ninth Circuit stated that, in United States v. Carey,

the Tenth Circuit suppressed evidence found when an officer, who was supposed to be searching a computer for drug-related documents, stumbled upon child pornography and began to search for more. Id. at 1276. Based on the officer's own testimony, the court found that the child pornography was not "inadvertently discovered" because the officer had temporarily abandoned the search authorized by the warrant in order to look for child pornography, contravening the limitations



of the search warrant. Id. at 1273. The court was careful to state that the result in the case (suppression of the evidence) was “predicated only upon the particular facts of this case, and a search of computer files based on different facts might produce a different result.” Id. at 1276 (footnote omitted). A concurring opinion stated that “if the record showed that [the officer] had merely continued his search for drug-related evidence and, in doing so, continued to come across evidence of child pornography, . . . a different result would be required.” Id. at 1277 (Baldock, B., concurring).

As the district court concluded, this case “is vastly different from Carey.” [The agent] was authorized to look at images and photographs; after discovering the pornographic images, [the agent] continued with his search for evidence of fake I.D. documents and only inadvertently came across more child pornography. The government only searched for pornographic files after obtaining the third search warrant authorizing it to do so, and the search was therefore reasonable.

527 F.3d at 891.

The Seventh Circuit reached a similar conclusion in United States v. Mann, 593 F.3d 779 (7th Cir. 2010). In United State v. Mann, officers received a warrant to search the defendant’s residence for “video tapes, CD’s or other digital media, computers, and the contents of said computers, tapes, or other electronic media, to search for images of women in locker rooms or other private areas.” 592 F.3d at 781-82. While searching one of the defendant’s computers, a detective discovered child pornography images and continued searching the computer for evidence of voyeurism. See 592 F.3d at 781. The detective ultimately discovered “many, many images of child pornography” on the defendant’s computer while conducting his original warrant-authorized search. 592 F.3d at 781.

The Seventh Circuit, in an opinion that Judge Rovner authored, and Judges Evans and Tinder joined, found that the detective did not exceed the scope of the search warrant when he continued searching the defendant’s computer for evidence that the search warrant sought. See 592 F.3d at 786. The Seventh Circuit distinguished the case from United States v. Carey on two grounds. See 592 F.3d at 783-84. First, the Seventh Circuit explained that, unlike the search

warrant in United States v. Carey, which was limited to “documentary” evidence of drug dealing, the search warrant in this case authorized the officers to search the defendant’s computer for images. 592 F.3d at 783-84. Second, the Seventh Circuit asserted that, unlike the detective in United States v. Carey, who “made clear as he opened each of the JPG files he was not looking for evidence of drug trafficking” and had “abandoned that search to look for child pornography,” the detective in this case testified that, at all times during the search, he “continued to look for items with voyeurism.” 592 F.3d at 783. In the Seventh Circuit’s view, therefore, the detective’s actions were much closer to the search that the Ninth Circuit found permissible in United States v. Wong, than the search that the Tenth Circuit found impermissible in United States v. Carey. See 592 F.3d at 783-84 (citing United States v. Wong, 334 F.3d at 835, 837-38). The Seventh Circuit noted, however, that the detective’s “failure to stop his search and request a separate warrant is troubling.” United States v. Mann, 592 F.3d at 786 (citing United States v. Burgess, 576 F.3d at 1055).

To be sure, multiple United States Courts of Appeals have upheld searches where executing officers immediately stopped their warrant-authorized searches upon discovering evidence of an unrelated crime. See, e.g., United States v. Lucas, 640 F.3d 168, 180 (6th Cir. 2011)(upholding denial of motion to suppress where officer obtained consent to search the defendant’s computer for evidence of drug trafficking and, upon discovering evidence of child pornography, immediately stopped searching until he obtained a search warrant for child pornography); United States v. Koch, 625 F.3d 470, 476 (8th Cir. 2010)(upholding search where officers immediately stopped their warrant-authorized search of the defendant’s flash drive for evidence of gambling when they discovered child pornography). The Court has been unable to find, however, a case in which a United States Court of Appeals has found continuing a

warrant-authorized computer search impermissible.

Third, such a rule would be inappropriate in cases where time is of the essence for the officer executing the original search warrant. For example, if a child is kidnapped and an officer obtains a warrant to search a computer for evidence of the child's condition or whereabouts, requiring the executing officer to stop searching the computer every time he or she discovers evidence of another crime would take valuable time away from the search effort. Similarly, where an officer obtains a warrant to search a computer for evidence of the location of a terrorist cell or weapons cache, forcing that officer to stop his or her search to obtain another warrant every time he or she discovers evidence of another crime could have catastrophic consequences. In these situations, officers should be allowed to continue their warrant-authorized computer searches even when they encounter evidence of another crime.

Where officers have ample time to pause their warrant-authorized search to obtain another warrant, however, Tenth Circuit precedent appears to require them to do so. As evidenced by the fact that Nishida did not open Loera's laptop to search it pursuant to the First Warrant until November 28, 2012, time was not of the essence in this case. Nishida conceded as much when he testified that it would not have been impractical to seize the CDs and other media that the agents discovered at Loera's residence to examine them at the FBI laboratory. See May 21, 2014 Tr. at 255:14-21 (Nishida, Serna). Consequently, there was nothing preventing the agents from sealing or holding Loera's items "pending approval by a magistrate of the conditions and limitations on a further search through the documents" for child pornography. United States v. Carey, 172 F.3d at 1275. The Court finds, therefore, that, under Tenth Circuit law, the agents conducted an unlawful search when they continued searching Loera's CDs upon discovering child pornography. The Court holds, accordingly, that the agents conducted an unlawful search

when they continued searching for evidence of computer fraud and electronic mail hijacking after discovering child pornography.

**V. THE AGENTS ACTED IN GOOD FAITH WHEN THEY CONTINUED TO SEARCH LOERA'S CDS FOR EVIDENCE OF ELECTRONIC MAIL HIJACKING AND COMPUTER FRAUD AFTER DISCOVERING CHILD PORNOGRAPHY.**

The agents acted in good faith when they continued to search Loera's CDs for evidence of electronic mail hijacking and computer fraud after discovering child pornography. "The fact that a Fourth Amendment violation occurred . . . does not necessarily mean that the exclusionary rule applies." United States v. Herring, 555 U.S. at 140 (citations omitted). The Supreme Court has stated that the exclusion of evidence "has always been our last resort, not our first impulse." Herring v. United States, 555 U.S. at 140 (citations omitted)(internal quotation marks omitted). The "sole purpose" of the exclusionary rule "is to deter future Fourth Amendment violations." United States v. Davis, 131 S. Ct. at 2426. In United States v. Davis, the Supreme Court emphasized that the goal of deterrence must be balanced against

the substantial social costs generated by the rule. Exclusion exacts a heavy toll on both the judicial system and society at large. It almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence. And its bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment. Our cases hold that society must swallow this bitter pill when necessary, but only as a last resort. For exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs.

131 S. Ct. at 2427. The Supreme Court further explained that "[t]he basic insight of the Leon line of cases is that the deterrence benefits of exclusion vary with the culpability of the law enforcement conduct at issue." 131 S. Ct. at 2427. Consequently, "[w]hen the police exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs." United States v. Davis,

131 S. Ct. at 2438 (citation omitted). By contrast, “[w]hen the police act with an objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence, the deterrence rationale loses much of its force, and exclusion cannot pay its way.” United States v. Davis, 131 S. Ct. at 2427-28 (citations omitted)(internal quotation marks omitted).

In United States v. Davis, the Supreme Court faced the issue whether the good-faith exception applied “when the police conduct a search in objectively reasonable reliance on binding judicial precedent.” 131 S. Ct. at 2428. The Supreme Court stated that “[u]nder our exclusionary-rule precedents, th[e] acknowledged absence of police culpability dooms Davis’s claim.” 131 S. Ct. at 2428. “Indeed, in 27 years of practice under Leon’s good-faith exception, we have never applied the exclusionary rule to suppress evidence obtained as a result of nonculpable, innocent police conduct.” 131 S. Ct. at 2428. Because “all that exclusion would deter in this case is conscientious police work,” the Supreme Court concluded that the good-faith exception applied. 131 S. Ct. at 2429.

**A. THE AGENTS REASONABLY RELIED ON BINDING APPELLATE PRECEDENT WHEN THEY CONTINUED THEIR WARRANT-AUTHORIZED SEARCHES AFTER FINDING CHILD PORNOGRAPHY.**

In United States v. Aguiar, 737 F.3d 251 (2d Cir. 2013), the Second Circuit addressed whether the good-faith exception applied to a police officer’s warrantless installation of a Global Positioning System (“GPS”) device to a suspect’s car before the Supreme Court’s decision in United States v. Jones, 132 S. Ct. 945 (2012), which found such installations unconstitutional. See United States v. Aguiar, 737 F.3d at 259-62. In an opinion that Judge Pooler wrote, and Judges Jacobs and Hall joined, the Second Circuit began its analysis by “addressing what is binding appellate precedent within the meaning of Davis.” 737 F.3d at 261. The Second Circuit

explained that, “[p]rior to Jones,” it “lacked occasion to opine on the constitutionality of using electronic tracking devices attached to vehicles, either of the beeper or GPS variety.” 737 F.3d at 261. The Second Circuit noted, however, that “the Supreme Court did have occasion to address the issue in both Knotts and Karo.” 737 F.3d at 261. The Second Circuit stated:

The Supreme Court’s decision in Knotts stood for the proposition that the warrantless use of a tracking device to monitor the movements of a vehicle on public roads did not violate the Fourth Amendment. 460 U.S. at 281-82, 285 . . . . Further, Karo discounted the importance of trespass in placing a device, stating that “a physical trespass is only marginally relevant to the question of whether the Fourth Amendment has been violated.” 468 U.S. at 712-13 . . . . Karo’s *de minimis* treatment of the trespass issue gave no indication that the issue of trespass would become the touchstone for the analysis in Jones. Moreover, Karo’s brushing off of the potential trespass fits logically with earlier Supreme Court decisions concluding that “the physical characteristics of an automobile and its use result in a lessened expectation of privacy therein.” New York v. Class, 475 U.S. 106, 112 . . . (1986). Nor is there an expectation of privacy when a car “travels public thoroughfares where its occupants and its contents are in plain view,” Cardwell v. Lewis, 417 U.S. 583, 590 . . . (1974). Taken together, law enforcement could reasonably conclude placing a GPS device on the exterior of Aguiar’s vehicles did not violate the Fourth Amendment.

Moreover, we find the beeper technology used in Knotts sufficiently similar to the GPS technology deployed by the government here. See, e.g., Sparks, 711 F.3d at 66 (finding defendants failed to distinguish in any substantive way how the installation of a beeper differed from the installation of a GPS device). Like the device at issue in Knotts, the GPS device allows law enforcement to conduct the same sort of surveillance it could conduct visually, but in a more efficient and cost-effective manner. Appellants argue that the GPS surveillance here continued over a period of months, tantamount to the sort of “dragnet type law enforcement practices” the Knotts court specifically declined to address. Knotts, 460 U.S. at 284 . . . . But the record indicates that the GPS device was used to track Aguiar’s vehicles on public thoroughfares, with technology undertaking an activity that police officers would have physically performed in the past. “Insofar as respondent’s complaint appears to be simply that scientific devices such as the beeper enabled police to be more effective in detecting crime, it simply has no constitutional foundation.” Id.

United States v. Aguiar, 737 F.3d at 261-62. The Second Circuit held, accordingly, that “at the time the GPS tracking device was applied to Aguiar’s car in January 2009, law enforcement could reasonably rely on that binding appellate precedent” and, therefore, the good-faith

exception applied. 737 F.3d at 261.

Following the Second Circuit's analysis in United States v. Aguiar, the Court first determines whether there existed any "binding appellate precedent" on which the agents could reasonably rely when they continued their search -- pursuant to the First Warrant -- for electronic mail hijacking and computer fraud after discovering child pornography. United States v. Aguiar, 737 F.3d at 261. "Binding appellate precedent" refers to both Tenth Circuit and Supreme Court precedent. United States v. Aguiar, 737 F.3d at 261. The Court first notes that there is no binding Tenth Circuit authority that addresses whether law enforcement officers may continue their warrant-authorized ESI searches upon discovering evidence of another crime. The Tenth Circuit has, instead, sent conflicting signals on whether such conduct is constitutional. Compare United States v. Carey, 172 F.3d at 1277 (Baldock, J., concurring)("[I]f the record showed that Detective Lewis had merely continued his [warrant-authorized] search for drug-related evidence, and, in doing so, continued to come across evidence of child pornography, I think a different result would be required."), with United States v. Walser, 275 F.3d at 987 ("Had [the officer] conducted a more extensive search than he did here by rummaging in folders and files beyond those he searched, he might well have exceeded the bounds of the warrant and the requirements of Carey")(emphasis added), and United States v. Burgess, 576 F.3d at 1094-95 ("[A]s our cases seem to require, [the officer] immediately closed the gallery view when he observed a possible criminal violation outside the scope of the warrant's search authorization and did not renew the search until he obtained a new warrant")(emphasis added). The Court's ruling that Nishida and Cravens conducted unlawful searches when they continued to search Loera's CDs after discovering child pornography was based on an analysis of non-binding Tenth Circuit dicta. Consequently, the agents could not rely on binding Tenth Circuit precedent when they continued

to search Loera's CDs for evidence of computer fraud and electronic mail hijacking after discovering child pornography.

Although the Supreme Court has never addressed the precise question here -- whether an officer may continue his or her warrant-authorized search for ESI upon discovering evidence of an unrelated crime -- it has upheld similar searches outside of the ESI context. In Horton v. California, an officer obtained a warrant to search the defendant's house for the proceeds of a robbery. See 496 U.S. at 131. While executing the search warrant, the officer found, and subsequently seized, among other things, a machine gun, a .38-caliber revolver, two "stun guns," and a handcuff key. 496 U.S. at 131. The officer did not find, however, any evidence that the search warrant sought. See 496 U.S. at 131. The officer testified that, while executing the search warrant, he was also looking for evidence outside the search warrant's scope. See 496 U.S. at 131. Finding the officer's subjective intentions during the search irrelevant, the Supreme Court explained:

[E]venhanded law enforcement is best achieved by the application of objective standards of conduct, rather than standards that depend upon the subjective state of mind of the officer. The fact that an officer is interested in an item of evidence and fully expects to find it in the course of a search should not invalidate its seizure if the search is confined in area and duration by the terms of a warrant.

496 U.S. at 138. Because the items seized "were discovered during a lawful search authorized by a valid warrant," and their seizure was justified by the plain-view exception, the Supreme Court found the officer's search constitutional. 496 U.S. at 142. Relying on the Supreme Court's precedent in Horton v. California, the agents could reasonably have concluded that the First Warrant permitted them to continue searching Loera's CDs after discovering child pornography. The Supreme Court all but encouraged officers to continue their warrant-authorized searches upon finding evidence of another crime by placing a single restriction on



officers who execute search warrants: that they may search only items that may reasonably contain the evidence that the warrant seeks. See Horton v. California, 496 U.S. at 142 (“Police with a warrant for a rifle may search . . . places where rifles might be and must terminate the search once the rifle is found; the inadvertence rule will in no way reduce the number of places into which they may lawfully look.”). Consequently, the agents could have reasonably relied upon Horton v. California to conclude that the First Warrant authorized them to continue searching Loera’s CDs for evidence of computer fraud and electronic mail hijacking, because those CDs could reasonably have contained evidence of those crimes.

The Court recognizes that “the storage capacity of computers” may require “a special approach,” United States v. Carey, 172 F.3d at 1275 n.7, and that Horton v. California is, therefore, not a perfect analogy. The Court notes, however, that the good-faith inquiry does not require officers to undertake the role of a judge or constitutional law scholar, and discern the precise contours of Supreme Court precedent. It instead turns on whether a reasonable officer would believe in good faith that binding appellate precedent authorized certain conduct, “which is a scenario-specific way of asking the broader question of whether the officer ‘acted with an objectively reasonable good-faith belief that his conduct was lawful.’” United States v. Katzin, No. 12-2548, 2014 WL 4851779 (3d Cir. Oct. 1, 2014)(en banc)(Van Antwerpen, J., joined by Rendell, Fisher, Charages, Jordan, Hardiman, Vanaskie, & Shwartz, JJ.). Viewed in this way, the Supreme Court’s holding in Horton v. California was sufficiently analogous to the agents’ circumstances for them to reasonably rely on it in continuing to conduct their warrant-authorized searches after finding child pornography. Consequently, the Court concludes that the good-faith exception applies to the agents’ conduct and suppression of the child pornography evidence obtained therefrom is unwarranted.

**B. EVEN IF THE AGENTS DID NOT REASONABLY RELY ON BINDING APPELLATE PRECEDENT, THE GOOD-FAITH BALANCING TEST WEIGHS AGAINST EXCLUDING THE EVIDENCE.**

Even if Horton v. California is not “binding appellate precedent” under United States v. Davis, the Court may still apply the good-faith exception, because the Tenth Circuit has not limited the good-faith exception to the factual circumstances that the Supreme Court has addressed. In United States v. McCane, 573 F.3d 1037 (10th Cir. 2009), for example, the Tenth Circuit, in an opinion that Judge Murphy authored, and Judges Anderson and Tymkovich joined, held, prior to the Supreme Court’s holding in United States v. Davis, that “[a] police officer who undertakes a search in reasonable reliance upon the settled case law of a United States Court of Appeals, even though his search is later deemed invalid by Supreme Court decision, has not engaged in misconduct.” 573 F.3d at 1045 (footnote omitted). Despite a lack of Supreme Court precedent on the issue indicating that the good-faith exception applied in situations where an officer acts in reasonable reliance on binding appellate precedent, the Tenth Circuit concluded that “[t]he refrain in Leon and the succession of Supreme Court good-faith cases is that the exclusionary rule should not be applied to objectively reasonable law enforcement activity.” 573 F.3d at 1045-46 (citations omitted)(internal quotation marks omitted). In the Tenth Circuit’s view, “[r]elying upon the settled case law of a United States Court of Appeals certainly qualifies as objectively reasonable law enforcement behavior.” 573 F.3d at 1045-46.

Other Circuits have followed a similar approach. In United States v. Davis, 690 F.3d 226 (4th Cir. 2012),<sup>13</sup> for example, the Fourth Circuit, in an opinion that Judge Agee authored, and Judge Keenan joined, held that the exclusionary rule did not apply where officers engaged in an

---

<sup>13</sup>Aside from the fact that both cases address the good-faith exception to the exclusionary rule, the United States v. Davis that the Fourth Circuit decided in 2012 is not related to the United States v. Davis that the Supreme Court decided in 2011.

unconstitutional search by extracting and testing the defendant's DNA sample during a murder investigation without a warrant. See 690 F.3d at 251-57. The Fourth Circuit determined that the Supreme Court's "recent decisions" applying the exclusionary rule "have broadened its application, and lead [the Fourth Circuit] to conclude that the Fourth Amendment violations here should not result in application of the exclusionary rule." 690 F.3d at 251. The Fourth Circuit explained:

Contrary to the dissent's contention, we are not creating a "new, freestanding exception" to the exclusionary rule. Rather, we have faithfully applied the Supreme Court's precedent, including its recent application of Leon in Herring and Davis. While the dissent refers to the "narrow holding[s]" in those cases, and deems inapplicable the "broad cost-benefit analysis" that underlies those holdings, . . . the Supreme Court's analysis in those cases is not dicta, but is the rationale supporting the Court's application of the good-faith exclusion.

United States v. Davis, 690 F.3d at 258 n.34.

The Third Circuit reached a similar conclusion in United States v. Katzin, a case decided by the Third Circuit en banc. In an opinion that Judge Van Antwerpen authored, the Third Circuit rejected the defendant's argument that the good-faith exception turned on whether the Supreme Court's decision in United States v. Davis applied. The Third Circuit explained:

The whole of our task is not to determine whether Davis applies, nor to "extend" either the good faith exception or Davis' holding. Even where Davis does not control, it is our duty to consider the totality of the circumstances to answer the "objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal." Leon, 468 U.S. at 906-07, 922 n.23. . . . To exclude evidence simply because law enforcement fell short of relying on binding appellate precedent would impermissibly exceed the Supreme Court's mandate that suppression should occur in only "unusual" circumstances: when it "further[s] the purposes of the exclusionary rule." Id. at 918. . .

Davis supports this conclusion. In reaching its holding, Davis reiterates the analytical steps for evaluating suppression challenges. 131 S. Ct. at 2426-28. For example, we must limit operation of the exclusionary rule "to situations in which [its] purpose," deterring future Fourth Amendment violations, is "most efficaciously served." Id. at 2426 . . . . Our analysis must account for both "[r]eal

deterrent value” and “substantial social costs,” and our inquiry must focus on the “flagrancy of the police misconduct” at issue. Id. at 2427 . . . . Only when, after a “rigorous weighing,” we conclude that “the deterrence benefits of suppression . . . outweigh its heavy costs,” is exclusion appropriate. Id. Importantly, we must be prepared to “appl[y] this ‘good-faith’ exception across a range of cases.” Id. at 2428.

Davis did not begin, nor end, with binding appellate precedent. Rather, binding appellate precedent informed -- and ultimately determined -- the Supreme Court’s greater inquiry: whether the officers’ conduct was deliberate and culpable enough that application of the exclusionary rule would “yield meaningfu[l] deterrence,” and “be worth the price paid by the justice system.” Id. at 2428 . . . . We must conduct the same analysis on the facts before us, even in the absence of binding appellate precedent.

United States v. Katzin, 2014 WL 4851779, at \*9-10 (citations omitted).

The Court agrees with the Third Circuit that “[t]o exclude evidence simply because law enforcement fell short of relying on binding appellate precedent” would violate “the Supreme Court’s mandate that suppression should occur in only ‘unusual’ circumstances: when it ‘furthers the purposes of the exclusionary rule.’” United States v. Katzin, 2014 WL 4851779, at \*9 (quoting United States v. Leon, 468 U.S. at 918). Accordingly, the Court must determine whether “the deterrence benefits” of suppressing the child pornography evidence “outweigh its heavy social costs.” United States v. Davis, 131 S. Ct. at 2427 (citations omitted). This balancing test is informed by the Supreme Court’s discussion in United States v. Davis, which indicates that the Court’s primary focus in evaluating the deterrence value in a particular case is on the culpability of the law enforcement officers who executed the search or seizure. As the Supreme Court explained, “[w]hen police exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs.” 131 S. Ct. at 2438 (citation omitted)(internal quotation marks omitted). By contrast, “when the police act with an objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence, the

deterrence rationale loses much of its force, and exclusion cannot pay its way.” United States v. Davis, 131 S. Ct. at 2427-28 (citations omitted)(internal quotation marks omitted). Based on: (i) the agents’ actions, which were, at most, negligent; and (ii) the unanimous opinion of the other Courts of Appeals to face this issue, which have uniformly upheld the constitutionality of the agents’ conduct, the Court concludes that the deterrence value of excluding the child pornography evidence is low. Moreover, given: (i) the large volume of child pornography evidence that would be suppressed in this case; and (ii) that the evidence plays a central role in the United States’ case, the Court determines that the social costs of excluding the evidence in this case would be relatively high. The Court holds, accordingly, that the good-faith balancing test weighs against suppressing the child pornography evidence.

**1. The deterrence value of excluding the child pornography evidence is low.**

The deterrence value of excluding the child pornography evidence in this case is low for three reasons. First, the Court cannot soundly conclude that Cravens’ and Nishida’s actions “exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights.” United States v. Davis, 131 S. Ct. at 2438 (citation omitted). Their actions reflect, at most, isolated negligence or ignorance of the subtleties of Tenth Circuit law. This search was not a general warrantless one in which the agents rummaged through Loera’s possessions for child pornography. Both agents reasonably concluded that the First Warrant authorized them to open all of the image files on Loera’s CDs. See May 20, 2014 Tr. at 53:7-11 (Cravens, Tuckman); id. at 152:6-8 (Nishida, Tuckman); id. at 160:5-11 (Nishida, Tuckman). Had the agents opened every file on every CD on which they found child pornography, their conduct may have been “deliberate, reckless or grossly negligent,” United States v. Davis, 131 S. Ct. at 2438 (citation omitted), but the agents did no such thing. When Cravens found child pornography on one of

Loera's CDs, he immediately ejected the CD and set it aside. See May 20, 2014 Tr. at 139:18-140:1 (Cravens, Court). When Nishida found child pornography on a different CD, he clicked on two or three other files on that CD to see if they contained any evidence of computer fraud or electronic mail hijacking, ejected the CD, and set it aside. See May 20, 2014 Tr. at 161:17-162:18 (Nishida, Tuckman). Moreover, at no point did either agent abandon their warrant-authorized searches to begin searching for child pornography. That nine of the thirteen CDs which the agents seized from Loera's residence had evidence of computer fraud and electronic mail hijacking indicates that the agents reasonably believed that a continued search of Loera's CDs after they discovered child pornography would uncover evidence that the First Warrant sought. Consequently, rather than acting with "deliberate, reckless, or grossly negligent disregard" for Loera's Fourth Amendment rights, United States v. Davis, 131 S. Ct. at 2438 (citation omitted), the agents' actions demonstrate that they were attempting to respect Loera's rights while continuing to execute their warrant-authorized searches.

Second, the agents reasonably could have interpreted the legal precedent on this issue -- both in the Tenth Circuit and nationwide -- as permitting them to continue searching Loera's CDs for evidence of computer fraud and electronic mail hijacking. Although the Court determined that the Tenth Circuit's statements, in dicta, in United States v. Walser and United States v. Burgess more accurately reflected existing Tenth Circuit law on computer searches than Judge Baldock's concurrence in United States v. Carey did, given the opacity of the Tenth Circuit precedent on this question, the agents could reasonably have reached the opposite conclusion.

The agents also could have reasonably relied upon the non-binding decisions of the United States Courts of Appeals that have addressed this issue, all of which have found similar

searches constitutional. See United States v. Peltier, 422 U.S. 531, 540-42, 540 n.8 (1975)(holding exclusionary rule inapplicable where illegal search was conducted in good faith reliance on, in part, holdings and dicta of various courts of appeals).<sup>14</sup> Specifically, the Third, Fourth, Seventh, Ninth, and Eleventh Circuits have all held that law enforcement officers may continue a warrant-authorized computer search upon discovering evidence of another crime. See United States v. Stabile, 633 F.3d at 240 (upholding denial of motion to suppress where officers continued warrant-authorized search of the defendant’s computer for financial crimes after discovering child pornography); United States v. Mann, 593 F.3d at 783-86 (upholding search where the officer continued his warrant-authorized search of the defendant’s computer for evidence of voyeurism after discovering child pornography); United States v. Williams, 592 F.3d at 521-24 (upholding search where the officer continued his warrant-authorized search of the defendant’s computer for evidence of “making threats and computer harassment” after discovering child pornography); United States v. Miranda, 325 F. App’x at 859-60 (per curiam)(upholding search where officer continued his warrant-authorized search for evidence of counterfeit software after discovering child pornography); United States v. Wong, 334 F.3d at 835 (upholding denial of motion to suppress where the officer continued his warrant authorized search of the defendant’s computer for, among other things, “[a]ny maps, receipts, or writings, depicting Churchill County Nevada” after discovering child pornography). All of these cases were decided before the agents searched Loera’s CDs on November 20, 2012. By considering these non-binding decisions in its good-faith analysis, the Court follows the good-faith analysis that the Supreme Court used in United States v. Peltier. In that case, the Supreme Court

---

<sup>14</sup>Although United States v. Peltier came before the Supreme Court’s ruling in United States v. Leon, the Supreme Court noted, in United States v. Davis, that United States v. Leon “explicitly relied on Peltier and imported its reasoning into the good-faith inquiry.” United States v. Davis, 131 S. Ct. at 2431-32.

considered the “constitutional norm” established by the United States Courts of Appeals to determine whether an officer “had knowledge, or [could] properly be charged with knowledge, that [a] search was unconstitutional under the Fourth Amendment.” 422 U.S. at 542. The Supreme Court stated that, “unless we are to hold that parties may not reasonably rely upon any legal pronouncement emanating from sources other than this Court, we cannot regard as blameworthy those parties who conform their conduct to the prevailing . . . constitutional norm.” 422 U.S. at 542. The Honorable Frank H. Easterbrook, United States Circuit Judge for the Seventh Circuit, has similarly observed:

[P]olice and the FBI (or lawyers advising them) often rely on precedent from one circuit when another has yet to address a question. One can doubt that much deterrence is to be had from telling the police that they are not entitled to rely on decisions issued by several circuits, just because the circuit covering the state in which [the investigation occurred] lacks its own precedent.

United States v. Brown, 744 F.3d 474 (7th Cir. 2014)(Easterbrook, J., joined by Kanne, & Tinder, JJ.).

The Court recognizes that excluding evidence where law enforcement officers conduct searches or seizures in the absence of binding appellate precedent would have some deterrent value. Doing so would be perhaps the most expedient way to educate law enforcement about the existence of a new constitutional rule. It would prevent law enforcement from engaging in aggressive readings of non-binding authority and force them to err on the side of caution in the face of constitutional uncertainty. It would likely even encourage law enforcement officers to follow closely the Fourth Amendment cases coming from the Tenth Circuit. In the Court’s view, however, excluding evidence not because of any culpable conduct, but instead to educate law enforcement officers about a new rule in Fourth Amendment jurisprudence, runs counter to the Supreme Court’s good-faith jurisprudence. See, e.g., United States v. Davis, 131 S. Ct. at 2429



(“Indeed, in 27 years of practice under Leon’s good-faith exception, we have never applied the exclusionary rule to suppress evidence obtained as a result of nonculpable, innocent police conduct.”)(citations omitted)(internal quotation marks omitted)).

Instead, analyzing whether the officer’s conduct was objectively reasonable in light of the existing authority -- both binding and non-binding -- at the time the officer conducted the search or seizure, addresses these concerns while respecting the Supreme Court’s good-faith analysis. Under that framework, where the officer’s interpretation of the existing authority constitutes a “deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights,” suppression may be warranted to deter that conduct. United States v. Davis, 131 S. Ct. at 2427 (citations omitted)(internal quotation marks omitted). On the other hand, where the officers act in objectively reasonable good-faith reliance on the existing authority, the deterrent effect of exclusion in such a case “can only be to discourage the officer from doing his duty.” United States v. Davis, 131 S. Ct. at 2429. In United States v. Katzin, the Third Circuit reached a similar conclusion, stating:

No doubt, sometimes officers’ reliance on non-binding authorities will fall short of an “objectively reasonable” good faith belief in the legality of their conduct. Suppression may then be appropriate to deter such reliance. It is equally elementary that close cases will be difficult. But in many other cases, law enforcement will likely correctly conclude, based upon a panoply of non-binding authority establishing a “constitutional norm,” Peltier, 422 U.S. at 542, that a particular police practice does not violate the Fourth Amendment. The value in deterring such conduct is low.

United States v. Katzin, 2014 WL 4851779, at \*16 (footnotes omitted). As the Third Circuit explained: “The boundaries of the good faith exception are a sufficient deterrent . . . . Law enforcement personnel will either tread cautiously or risk suppression.” United States v. Katzin, 2014 WL 4851779, at \*17 (citations omitted). Given that every other United States Court of Appeals to confront this issue has upheld the agents’ conduct, it was reasonable for the agents to

conclude that continuing their warrant-authorized searches upon discovering child pornography was constitutional. The agents' actions are, therefore, closer to the cases of "simple, isolated negligence," where "exclusion cannot pay its way," than the "deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights" that the exclusionary rule is designed to deter. United States v. Davis, 131 S. Ct. at 2427-28, 38 (citations omitted)(internal quotation marks omitted).

Because of the agents' testimony that they believed that the First Warrant authorized them to continue searching for evidence of computer fraud and electronic mail hijacking after they discovered child pornography, because of the lack of clarity in Tenth Circuit precedent on this issue, and because every United States Courts of Appeals to address this issue has approved of the agents' conduct, the Court concludes that the deterrence value of excluding the child pornography evidence in this case is low.

**2. The social costs of excluding the child pornography evidence in this case are high.**

The Supreme Court has stated that the good-faith analysis "must account for the substantial social costs generated by the [exclusionary] rule."<sup>15</sup> United States v. Davis, 131 S. Ct. at 2427. Aside from stating that exclusion exacts a "heavy toll on both the judicial system and society at large" by requiring courts "to ignore reliable, trustworthy evidence bearing on

---

<sup>15</sup>The Court has recognized that "both scholars and judges have posited that exclusion of probative, reliable evidence of a defendant's guilt is too high a price to pay for the unknown degree of deterrence that exclusion achieves." United States v. Christy, 785 F. Supp. 2d at 1039 n.8 (citing Christopher Slobogin, Why Liberals Should Chuck the Exclusionary Rule, 1999 U. Ill. L. Rev. 363, 369-70, 442-43 (1999); Akhil Reed Amar, Fourth Amendment First Principles, 107 Harv. L. Rev. 757, 795-800 ("[I]f deterrence is the key, the idea is to make the government pay, in some way, for its past misdeeds, in order to discourage future ones. But why should that payment flow to the guilty? Under the exclusionary rule, the more guilty you are, the more you benefit."); Hon. Malcolm Richard Wilkey, A Call for Alternatives to the Exclusionary Rule, 62 Judicature 351 (1978-79); Hon. Malcolm Richard Wilkey, The Exclusionary Rule: Why Suppress Valid Evidence?, 62 Judicature 214 (1978-79)).

guilt or innocence,” the Supreme Court has not articulated how a court should quantify the social costs of excluding evidence in a particular case. United States v. Davis, 131 S. Ct. at 2428 (citations omitted). See, e.g., United States v. Herring, 555 U.S. at 701 (“The rule’s costly toll upon truth-seeking . . . presents a high obstacle for those urging its application.”)(brackets omitted)(citation omitted)(internal quotation marks omitted); United States v. Leon, 468 U.S. at 907 (“Our cases have consistently recognized that unbending application of the exclusionary sanction . . . would impede unacceptably the truth-finding functions of judge and jury.”)(citation omitted)(internal quotation marks omitted); United States v. Ceccolini, 435 U.S. 268, 279 (1978)(Rehnquist, J., joined by Burger, Stewart, White, Powell, Stevens, JJ.) (“[W]hen balancing the interests involved, we must weigh the strong interest under any system of justice of making available for the trier of fact all concededly relevant and trustworthy evidence which either party seeks to adduce.”)(citations omitted)(internal quotation marks omitted); Rakas v. Illinois, 439 U.S. at 137 (“Each time the exclusionary rule is applied it exacts a substantial cost . . . . Relevant and reliable evidence is kept from the trier of fact and the search for truth at trial is deflected.”)(citations omitted); Stone v. Powell, 428 U.S. 465, 490 (1976)(Powell, J., joined by Burger, Stewart, Blackmun, Rehnquist, & Stevens, JJ.) (“[T]he physical evidence sought to be excluded is typically reliable and often the most probative information bearing on the guilt or innocence of the defendant . . . . Application of the [exclusionary] rule thus deflects the truthfinding process . . . .”).

United States v. Katzin, which the Third Circuit decided, is the only case to address what factors courts should consider in determining the social costs of applying the exclusionary rule. Rather than weighing the society-wide implications of excluding evidence, the Third Circuit focused on the amount of evidence that would be excluded in that case, and the effect of

exclusion on the government's case. See United States v. Katzin, 2014 WL 4851779, at \*17. The case was a robbery case and the defendant had moved to suppress the proceeds from the robbery that the police uncovered as a result of an unlawful search. See United States v. Katzin, 2014 WL 4851779, at \*2-3. The Third Circuit stated that, "by all appearances, the Government's evidence against [the defendant] is substantial, and it is uncontested that the Government would have no case without it. The costs of exclusion are high." United States v. Katzin, 2014 WL 4851779, at \*17.

To determine the social costs of excluding the child pornography evidence, the Court will follow the Third Circuit's approach in United States v. Katzin. If the Court were to use general societal costs -- rather than case-specific costs -- the costs of exclusion would likely always outweigh the benefits for those who dislike the exclusionary rule and the benefits would outweigh the costs where the court is favorable to the exclusionary rule; the analysis would, therefore, lack any principled rule. Accordingly, the Court will focus on: (i) the amount of reliable evidence that would be suppressed; and (ii) the role that such evidence would likely play in the United States' case.<sup>16</sup> In the Court's view, both of these factors indicate the social costs of

---

<sup>16</sup>It may be tempting to want to balance the severity of the crime in determining whether the good-faith exception applies -- to consider, for example, that exclusion may be less appropriate where the unlawful search or seizure uncovers evidence of a serious crime -- like officers discovering a group of severed heads in a suspect's home -- than where the unlawful search or seizure uncovers evidence of a minor crime -- like a joint of marijuana in a teenager's pocket. The Court has been unable to find, however, a case in which a court has considered this factor in its good-faith analysis. In the Court's view, that an act has been criminalized reflects the political process' determination of the cost of such behavior to society, and the courts should be reluctant to second guess that determination with its own ad hoc, personal preferences and individualized determination of the severity of the crime. The Court is also concerned that: (i) it would be difficult how to gauge the seriousness of an offense; (ii) it would be difficult to figure out how to factor this determination into the balancing test; (iii) weighing the seriousness of an offense may encourage law enforcement officers to conduct illegal searches and seizures while investigating serious crimes; and (iv) the balancing test should consider only the change in probability of conviction, not the conviction's consequences, because sentencing -- which is kept

excluding the child pornography evidence would be high.

First, exclusion would prevent the factfinder from considering a large volume of relevant and reliable evidence. Nishida found over 730 images and forty movies of child pornography on Loera's laptop -- so many that he eventually stopped counting them. See May 20, 2014 Tr. at 186:22-25 (Nishida, Tuckman); id. at 186:25-187:5. Nishida also discovered approximately 330 images and two movies of suspected child pornography on Loera's CDs. See Apr. 19, 2013, Examination Report at 2. The Court also has no reason to believe this evidence is unreliable. Forensic experts from the FBI obtained it, and there are no allegations anyone has altered or tampered with it in any way. Accordingly, granting suppression in this case would keep a staggering amount of relevant and reliable information from the factfinder.

Second, because the United States has charged Loera only with possession of child pornography, the United States would likely not have a case without the child pornography itself. See Superseding Indictment at 1-2, filed January 9, 2014 (Doc. 25) ("Superseding Indictment"). Although the Court does not purport to know the United States' trial strategy or what other evidence the United States has or will obtain during its investigation, by all appearances, the United States' case rests entirely on this child pornography evidence. These considerations indicate, therefore, that the costs of exclusion in this case would be high and case determinative.

Even if the Court focused solely on the broader, society-wide costs of applying the

---

strictly separate from the guilt/innocence determination in our system -- incorporates the severity of the crime. In the end, the Fourth Amendment protects privacy, and not certain criminal activity. Accordingly, the Fourth Amendment analysis should be the same, whether the crime includes an murder, illegal re-entry, drugs, firearms, or child pornography. Likewise, the exclusionary rule analysis should be the same for every crime. Once the political branches have said something is a crime, the courts should not choose whether to apply the exclusionary rule depending on the crime. Social costs, as the Supreme Court uses that term, should mean something else. For these reasons, the Court will not consider the severity of the crime in applying the good-faith balancing test.

exclusionary rule, it would conclude that the social costs are high and exclusion is unwarranted. The exclusionary rule “provides a remedy only for defendants where incriminating evidence was actually found against them -- those who are thus most likely to be actually guilty -- and fails to provide any remedy to citizens against whom unconstitutional searches were conducted where no such evidence was found -- those most likely to be actually innocent.” Tonja Jacobi, The Law and Economics of the Exclusionary Rule, 87 Notre Dame L. Rev. 585, 588 (2011). Consequently, the exclusionary rule’s “bottom-line effect, in many cases, is to . . . set the criminal loose in the community without punishment.” Davis v. United States, 131 S. Ct. at 2427 (citations omitted). Professor Richard E. Myers has noted that,

the cost of the exclusionary rule must also be accounted for in terms of judicial legitimacy -- when evidence is excluded, judges are seen as engaging in behavior other than a quest for the truth, and I would expect that while lawyers are ready to think about the other important roles the court plays as part of an overall system, the lay public is not.

Richard E. Myers II, Fourth Amendment Small Claims Court, 10 Ohio St. J. Crim. L. 571, 583 (2013). Given these considerations, the general societal costs of excluding the child pornography evidence would be high. Thus, whether the court focuses on the specific costs of applying the exclusionary rule in this case or the general societal costs of applying the exclusionary rule in all cases, the result here is the same: the costs of applying the exclusionary rule in this case are high.

Given the low deterrence value of excluding evidence where the agents’ actions constitute, at most, isolated negligence or excusable ignorance about the subtleties of Tenth Circuit law, and the high social costs of excluding child pornography evidence in a case involving the possession of child pornography, the Court concludes that the good-faith balancing test weighs against excluding the child pornography evidence.

**VI. THE FIRST WARRANT DID NOT PERMIT CRAVENS TO OPEN FILES ON LOERA’S CDS ON NOVEMBER 27, 2012, FOR THE LIMITED PURPOSE OF PROVIDING JUDGE SCHNEIDER A DESCRIPTION OF FOUR IMAGES DEPICTING CHILD PORNOGRAPHY IN HIS SEARCH WARRANT AFFIDAVIT.**

The First Warrant did not permit Cravens to open files on Loera’s CDs on November 27, 2012, for the limited purpose of providing Judge Schneider a description of four images depicting child pornography in the Second Affidavit. Loera argues that Cravens’ November 27, 2012, search of Loera’s CDs exceeded the First Warrant’s scope. See Memorandum at 10-11. Loera argues that “[t]hese . . . searches for child pornography were not within the scope of the November 19 warrant for evidence of wire fraud and unlawful interception of electronic communications.” Memorandum at 11. The United States concedes that, “[g]enerally, law enforcement engaged in a lawful search[,], who wish to abandon that search and begin a focused search for child pornography, need to obtain a search warrant before beginning a child pornography search.” Response at 11 (citations omitted).

“A Fourth Amendment search occurs either where the government, to obtain information, trespasses on a person’s property or where the government violates a person’s subjective expectation of privacy that society recognizes as reasonable to collect information.” Ysasi v. Brown, 2014 WL 936835, at \*8. See United States v. Jones, 132 S. Ct. at 947. “[T]he Katz reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.” United States v. Jones, 132 S. Ct. at 947 (emphasis in original)(citing Alderman v. United States; Soldal v. Cook Cnty.). “When ‘the Government obtains information by physically intruding’ on persons, houses, papers, or effects, ‘a ‘search’ within the original meaning of the Fourth Amendment’ has ‘undoubtedly occurred.’” Florida v. Jardines, 133 S. Ct. at 1414 (quoting United States v. Jones, 132 S. Ct. at 950 n.3).

The United States does not contest that Cravens searched Loera's CDs on November 27, 2012. The United States' position is that Cravens' "limited review of some files so that he could include a brief description in his affidavit did not rise to the level of an unlawful search outside the scope of the First Warrant." Response at 11. The United States does not cite -- and the Court has been unable to find -- a case in which a court has upheld a search for the limited purpose of providing a description of the items searched in a search warrant affidavit. The Court will not do so here.

At the suppression hearing, Cravens admitted that he searched Loera's CDs on November 27, 2012, for child pornography. See May 20, 2014 Tr. at 72:1-4 (Cravens); id. at 72:21-22 (Cravens). Cravens explained that, to find child pornography images that he could accurately describe in the affidavit, he looked at several images -- "more than just a couple" of images, but "[m]ost likely less than a dozen" -- on each of the four CDs. May 20, 2014 Tr. at 143:6-16 (Cravens, Court). On November 27, 2012, Cravens had the four CDs for a total of two-and-a-half hours, during which time he also drafted the Second Affidavit. See May 20, 2014 Tr. at 74:10-21 (Cravens, Tuckman).

Cravens' November 27, 2012, searches of Loera's CDs violated the Fourth Amendment. Cravens was not searching for evidence of electronic fraud and computer hijacking pursuant to the First Warrant. Instead, Cravens hoped to find child pornography, so that he could provide a description of the child pornography in his search warrant affidavit. See May 20, 2014 Tr. at 72:1-4 (Cravens); id. at 72:21-22 (Cravens). Because Cravens was not searching for evidence of electronic fraud and computer hijacking, his searches of Loera's CDs exceeded the scope of the First Warrant. Moreover, because exigent circumstances or any other exception to the warrant requirement did not justify his searches, they are unconstitutional. The Court will, accordingly,



excise paragraphs 23-27 of the Second Affidavit, as they are the fruit of Cravens' unlawful November 27, 2012, search.

**VII. ALTHOUGH CRAVENS WAS NOT PERMITTED TO OPEN FILES ON LOERA'S CDS ON NOVEMBER 27, 2012, TO PROVIDE A DESCRIPTION OF IMAGES ON THE CDS IN A SEARCH WARRANT AFFIDAVIT, PROBABLE CAUSE TO ISSUE THE SECOND WARRANT STILL EXISTED WITHOUT CRAVENS' DESCRIPTIONS OF THOSE IMAGES.**

Although Cravens was not permitted to open files on Loera's CDs on November 27, 2012, to provide a description of images on those CDs in the Second Affidavit, probable cause to issue the Second Warrant still existed without Cravens' descriptions of those images. The United States argues that, even without Cravens' description of the images and video that he saw on November 27, 2012, the Second Affidavit includes sufficient probable cause to properly obtain the Second Warrant. See Response at 14. The United States explains that Cravens stated in the Second Affidavit that: (i) he had been an FBI agent for eight years; (ii) his experience included investigations of "crimes against children on the Internet"; (iii) computers and electronic media -- including CDs -- are used in the child pornography industry; (iv) child pornography images were found on the four CDs seized from Loera's residence; and (v) when he used the term "child pornography," he meant "a visual depiction involving the use of minors engaged in sexually explicit conduct." Response at 12-13 (citations omitted). The United States further asserts that the Tenth Circuit has recognized that the phrase "child pornography" has a generally understood meaning and referring to images of child pornography provides sufficient probable cause to obtain a search warrant. Response at 13 (citing, e.g., United States v. Haymond, 672 F.3d at 959; United States v. Cervini, 16 F. App'x at 868). In the United States' view, the situation is similar to one in which a Drug Enforcement Agency agent is trying to obtain a warrant for a house, and explains in the warrant affidavit that he has been an agent for

twelve years, has extensive experience with drugs, and smelled the odor of marijuana coming from the home. See Aug. 19, 2014 Tr. at 336:4-17 (Tuckman). The United States argues that, accordingly, the information in the Second Affidavit -- even without descriptions of the images or videos on the CDs -- established sufficient probable cause for Judge Schneider to issue the Second Warrant. See Response at 14.

Loera contends that, after excising Cravens' unlawfully obtained descriptions from the Second Affidavit, the resulting affidavit would read, "four writable CDs . . . appeared to contain images of child pornography." Reply at 5. In Loera's view, "child pornography" is a "mere conclusory statement" that "cannot support probable cause." Reply at 6. In support of his argument, Loera points to United States v. Roach. See Aug. 19, 2014 Tr. at 335:15-19 (Serna). Loera contends that, accordingly, without the detailed description of the specific images and video that Cravens obtained from his November 27, 2012, search, the Second Affidavit does not establish probable cause. See Reply at 6. The Court agrees with the United States.

"When a search is conducted pursuant to a warrant that is based on illegally obtained information, a court is not to blindly apply the good-faith exception." United States v. Romero, 743 F. Supp. 2d at 1316. "An affidavit containing erroneous or unconstitutionally obtained information invalidates a warrant if that information was critical to establishing probable cause. If, however, the affidavit contained sufficient accurate or untainted evidence, the warrant is nevertheless valid." United States v. Christy, 785 F. Supp. 2d 1004, 1051, on reconsideration in part, 810 F. Supp. 2d 1219 (D.N.M. 2011). See United States v. Karo, 468 U.S. at 721 (finding that a search warrant affidavit, after striking facts obtained illegally, "contained sufficient untainted information to furnish probable cause for the issuance of the search warrant").

"In determining whether probable cause supported the issuance of a search warrant, we give 'great deference' to the decision of the issuing magistrate or

judge.” Cusumano, 83 F.3d at 1250 (quoting United States v. Williams, 45 F.3d 1481, 1485 (10th Cir. 1995)). We review only whether the issuing magistrate or judge had a “substantial basis” for finding probable cause, requiring “a practical, common sense decision whether, given all the circumstances set forth in the affidavit before him . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place. And the duty of the reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed.” Id.

United States v. Sims, 428 F.3d at 954.

In United States v. Sims, the Tenth Circuit affirmed the district court’s ruling that the warrants were based on probable cause without regard to the information gleaned by officers from prior warrantless searches, stating:

Here, in addition to the information coming from the warrantless office search, the affidavit contained detailed information about Sims’s contacts with Mike Walker and the FBI’s confirmation, after assuming the “sweetthingforyou16” identity, that Sims was planning to travel to meet Sue and Kate. The magistrate had information about the images sent to Walker, messages and images sent to the FBI, Sims’s detailed plans to go to Missouri to meet Sue and Kate, and that Sims used both his home and office computers to send these messages.

In this case, the depth of the affidavit’s specific information regarding Sims’s suspected activity was more than sufficient to warrant suspicion and give the magistrate judge a reasonable ground to believe relevant evidence would be found.

428 F.3d at 954.

In United States v. Cusumano, the Tenth Circuit found that the officer’s search warrant affidavit set forth “numerous facts in such detail that, in aggregate, lead us to conclude that a fair probability existed that Defendants were growing marijuana in the basement of their residence” and, thus, that “the search warrant was based on probable cause even without the information supplied by the thermal imager.” 83 F.3d at 1250. The officer had based his conclusion that the defendants were growing marijuana in the basement of their residence on the following verified facts: (i) the defendants stated to the landlord that a grow light in their furnace room was used to

grow fresh vegetables; (ii) the landlord detected a strong musty odor in the residence's basement; (iii) power company reports indicated that the residence was consuming twice the amount of electricity as similar structures in the area; (iv) an electrician whom the defendants had hired to approve electrical work in the residence's basement reported that the existing wiring could support a grow operation; (v) the defendants "received delivery of five hundred gallons of diesel fuel at the residence to operate the generator"; (vi) the defendants paid their rent in three-month installments of \$2,100.00 in cash; (vi) the defendants had no viable means of support; (vii) "Resident Thomas J. Sanatello (a defendant in the district court) refused to allow the landlord's homeowners insurance agent to inspect the residence for a two week period"; (viii) "the insurance agent observed two wheel barrows, a shovel, and sacks of soil near a door of the residence leading to the basement"; and (ix) the "insurance agent feared for his safety while speaking with Sanatello." 83 F.3d at 1248-49. The Tenth Circuit found that the "totality of the evidence substantially supports the conclusion that there was 'a fair probability that contraband or evidence of a crime' would be found in Defendants' home." 83 F.3d at 1247 (citation omitted).

In United States v. Christy, the Court excised unlawfully obtained information from a search warrant affidavit. See 785 F. Supp. 2d at 1052. The remaining information contained in the search warrant affidavit was: (i) the Westminster Police Department in California asked the Bernalillo County Sheriff's Office ("BCSO") to perform a welfare check at 2265 Kelly SW in Albuquerque in reference to a missing sixteen year-old female -- K.Y.; (ii) the Westminster Police Department told BCSO that K.Y. possibly left California with the defendant and gave BCSO K.Y.'s description and the defendant's address; (iii) K.Y. possibly left California because of electronic mail transmissions recovered from K.Y.'s account; (iv) these electronic mail

transmissions helped identify the defendant and contained two photographs which showed the defendant naked and which he sent of himself; and (v) the Westminster Police Department sent BCSO an electronic mail transmission that the defendant sent K.Y. on November 6, 2009, which indicated that the defendant knew K.Y. was sixteen years old. See 785 F. Supp. 2d at 1052-53.

The Court concluded:

Excluding the information illegally obtained, the warrants do not establish a fair probability that evidence of a crime would be found in Christy's home, vehicle, person, or cellular telephones. The remaining factual details in the warrants are bare. Given that the age of consent in New Mexico is sixteen, the Court does not believe that the remaining factual allegations support the conclusion that there was a fair probability that evidence of a crime would be found in Christy's home.

United States v. Christy, 785 F. Supp. 2d at 1053 (citation omitted).

"The Court must exclude the information illegally obtained from the warrants and determine whether, based on the remaining information, probable cause nevertheless existed." United States v. Christy, 785 F. Supp. 2d at 1051. With the descriptions of the three images and one video that Cravens obtained from his November 27, 2012, search of Loera's CDs excised, the remaining information in the Second Affidavit is: (i) Cravens had been an FBI agent for eight years, see Second Affidavit ¶ 2, at 1; (ii) Cravens' experience included investigations of "crimes against children on the Internet," Second Affidavit ¶ 2, at 1; (iii) in Cravens' experience, computers and electronic media -- including CDs -- are used to possess and distribute child pornography, see Second Affidavit, ¶¶ 8-14, at 3-6; (iv) during the execution of the First Warrant on November 20, 2012, child pornography images were found on the four CDs seized from Loera's residence, see Second Affidavit ¶ 21, at 8; and (v) when Cravens used the term "child pornography," he meant "a visual depiction involving the use of minors engaged in sexually explicit conduct," Second Affidavit, ¶ 30, at 10.

Even with Cravens' descriptions of the three images and one video from his November

27, 2012, search excised, the Second Affidavit contains sufficient probable cause. Probable cause exists when “there is a fair probability that contraband or evidence of a crime will be found in a particular place.” United States v. Simpson, 152 F.3d at 1246 (citations omitted). In United States v. Cervini, the Tenth Circuit addressed whether a search warrant in which a law enforcement officer states that he has viewed “child pornography” establishes probable cause. 16 F. App’x at 868-69. The Tenth Circuit stated:

Terry Wade, a Special Agent for the Federal Bureau of Investigation and former agent for the Oklahoma Bureau of Investigation, applied for a warrant to search Cervini’s residence, attaching a personal affidavit to the application in support of the warrant. The affidavit describes in some detail the process by which an individual may post a message to an Internet newsgroup and the manner in which the individual may be traced from his posting.

In addition, the affidavit includes details of the specific crime for which the search warrant was sought. Special Agent Wade indicated in his affidavit that two images of child pornography were posted to an Internet newsgroup just before 1:00 a.m. on April 27, 1999. The message header accompanying the transmission contained the Internet protocol (IP) address 206.154.188.85 and revealed that the message was posted from a news server owned by Innovative Technology, Ltd., an Internet service provider (ISP). The ISP’s records revealed that the account responsible for the posting had been in use for four hours and was not logged off until just before 3:00 a.m. In response to a grand jury subpoena, the ISP identified the account holder from the IP address as Michael Cervini. The ISP provided Cervini’s address and indicated that his customer account status was active. Cervini’s residential address was corroborated through both a records check of Southwestern Oklahoma State University and an Oklahoma driver’s license query.

16 F. App’x at 868-69. Finding that the information in the agent’s affidavit established probable cause, the Tenth Circuit reasoned that,

[t]he issuing judge reasonably could have inferred from the facts provided in the affidavit that (1) an individual is likely to generate child pornography in a location where he has the greatest expectation of privacy; (2) a computer would be found at an ISP subscriber’s residence; (3) Cervini was most likely at home at 1:00 a.m.; and (4) as the account holder, Cervini was the person using the account. Contrary to Cervini’s claim, these conclusions do not require the issuing judge to pile inference upon inference. The totality of the facts enable a reasonable person to

draw the common-sense conclusion that evidence of the crime would be found at Cervini's residence

16 F. App'x at 868-69.

As in United States v. Cervini, the Second Affidavit established probable cause. Because Cravens stated in the Second Affidavit that child pornography was discovered on the CDs seized from Loera's residence during the execution of the First Warrant, and because Cravens defined child pornography as "a visual depiction involving the use of minors engaged in sexually explicit conduct," Second Affidavit, ¶ 30, at 10, the Court concludes that the First Warrant indicated that there was "a fair probability that contraband or evidence of a crime will be found" on the media items seized from Loera's residence, United States v. Simpson, 152 F.3d at 1246. The Court holds, accordingly, that -- even with Cravens' descriptions of the three images and one video that he obtained from his November 27, 2012, searches excised from the Second Affidavit -- the Second Affidavit provided sufficient probable cause for Judge Schneider to properly issue a search warrant.

**VIII. EVEN IF THE SECOND WARRANT SUFFERED FROM AN INCURABLE DEFECT, NISHIDA RELIED ON THE WARRANT IN GOOD FAITH WHEN HE SEARCHED LOERA'S CDS AND LAPTOP FOR CHILD PORNOGRAPHY.**

Even if the Second Warrant suffered from an incurable defect, Nishida relied on the warrant in good faith when he searched Loera's CDs and laptop for child pornography. The United States asserts that Nishida searched Loera's laptop and CDs for child pornography only after Judge Schneider issued the Second Warrant. See Response at 16. In the United States' view, Nishida relied on Judge Schneider's determination that probable cause existed to search those items "reasonably and in good faith." Response at 16. The United States argues that, consequently, the Court should not suppress any evidence obtained through the execution of the Second Warrant. See Response at 16. The United States contends that Cravens also acted in

good faith in obtaining the Second Warrant. See Response at 15-16. The United States explains that, in the Second Affidavit, Cravens stated that he opened files on Loera's CDs on November 27, 2012, to provide a description of the files in his search warrant affidavit. See Response at 16. The United States points out that Cravens had Mr. Anderson, Assistant United States Attorney review his application for the Second Warrant, including the Second Affidavit. See Response at 4, 15. The United States argues that the Tenth Circuit has identified asking a lawyer to approve a search warrant application as one factor that indicates an officer acted in good faith in obtaining a warrant. See Response at 16 (citing United States v. Otero, 563 F.3d at 1134-35). The United States contends that Cravens' actions demonstrate that he "was trying to comply with the law," and are "not enough to justify exclusion." Response at 16. The United States argues that Judge Schneider was not misled by any falsehoods, and he remained neutral and detached. See Response at 15. The United States further contends that the Second Affidavit "overwhelmingly" established probable cause, and there was nothing on the face of the Second Warrant that would lead Nishida to presume it was invalid. Response at 15.

Loera asserts that the good-faith exception does not apply in this case. See Reply at 6-8. Loera argues that the First Affidavit was "so lacking in probable cause" to search for child pornography, image or video files, or any file with the date last modified before July 29, 2011, that the FBI agents' reliance on it was unreasonable. Reply at 7. Loera further states that "the government's second warrant on November 29 to search for child pornography after it had conducted two warrantless searches . . . also shows a lack of good faith." Reply at 7. Loera concludes his argument on the applicability of the good-faith exception by asserting:

Despite the existence of Carey, which stated in 1999 that a warrant should be acquired after the first image was seen, the government here proceeded to conduct more searching for child pornography on November 20 and on November 27 before finally seeking a search warrant on November 29 for child pornography.



Good faith did not exist.

Reply at 7-8. The Court agrees with the United States.

Even if the Second Affidavit did not contain sufficient probable cause, “[e]vidence seized pursuant to an invalid warrant does not necessarily have to be suppressed.” United States v. Riccardi, 405 F.3d at 863. The Supreme Court has explained that the “sole purpose” of the exclusionary rule “is to deter future Fourth Amendment violations.” United States v. Davis, 131 S. Ct. at 2426. Accordingly, where suppression “fails to yield appreciable deterrence, exclusion is clearly . . . unwarranted.” United States v. Davis, 131 S. Ct. at 2426-27 (alterations in original). “Where an officer acting with objective good faith obtains a search warrant from a detached and neutral magistrate and the executing officers act within its scope, there is nothing to deter.” United States v. Riccardi, 405 F.3d at 863 (quoting United States v. Nolan, 199 F.3d 1180, 1185 (10th Cir. 1999); United States v. Tuter, 240 F.3d 1292, 1298-99 (10th Cir. 2001)). “Thus, the evidence seized pursuant to such a warrant should not be excluded from trial.” United States v. Nolan, 199 F.3d at 1184. In cases in which officers obtained a search warrant,

an officer cannot be expected to question the magistrate’s probable-cause determination. . . . Once the warrant issues, there is literally nothing more the policeman can do in seeking to comply with the law. Penalizing the officer for the magistrate’s error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations.

United States v. Leon, 468 U.S. at 921 (citations omitted)(internal quotation marks omitted).

The Tenth Circuit has explained that, “[u]nder Leon, we presume good-faith when an officer acts pursuant to a warrant unless one of ‘four contexts’ apply.” United States v. Barajas, 710 F.3d at

1110

First, evidence should be suppressed if the issuing magistrate was misled by an affidavit containing false information or information that the affiant would have known was false if not for his “reckless disregard for the truth.” Second, the exception does not apply when the “issuing magistrate wholly abandon[s] his

judicial role.” Third, the good-faith exception does not apply when the affidavit in support of the warrant is “so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.” Fourth, the exception does not apply when a warrant is so facially deficient that the executing officer could not reasonably believe it was valid.

United States v. Danhauer, 229 F.3d at 1007 (quoting United States v. Leon, 468 U.S. at 922-23)(citations omitted). See United States v. Perrine, 518 F.3d 1196, 1206-07 (10th Cir. 2008). “If any of these situations is present, the good-faith exception should not be applied, and the evidence should be excluded.” United States v. Romero, 743 F. Supp. 2d at 1316.

Here, the only exception to the good-faith exception that could reasonably apply is that the Second Affidavit was “so lacking in indicia of probable cause as to render” the executing officer’s belief unreasonable. United States v. Danhauer, 229 F.3d at 1007 (citations omitted). The “threshold for establishing this exception is a high one,” Messerschmidt v. Millender, 132 S. Ct. 1235, 1245 (2012), and Loera has not overcome that burden here. The affidavit in this case is not a “bare bones” affidavit. Illinois v. Gates, 462 U.S. at 239. It does not rely on Cravens’ unsupported belief that probable cause exists. See Illinois v. Gates, 462 U.S. at 239 (identifying the affidavits in Nathanson v. United States and Aguilar v. Texas as “bare bones,” because each contained only an officer’s belief that probable cause existed without providing any factual details). Instead, the Second Warrant specifically identified child pornography as a “visual depiction involving the use of minors engaged in sexually explicit conduct” and was appropriately limited to evidence of child pornography. Second Affidavit ¶ 30, at 10. Moreover, the “deterrence benefits” of suppressing the child pornography evidence in this case “outweigh its heavy social costs.” United States v. Davis, 131 S. Ct. at 2427 (citations omitted). As the Supreme Court has explained: “When police exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to

outweigh the resulting costs.” United States v. Davis, 131 S. Ct. at 2438 (citation omitted). By contrast, “when the police act with an objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence, the deterrence rationale loses much of its force, and exclusion cannot pay its way.” United States v. Davis, 131 S. Ct. at 2427-28 (citations omitted)(internal quotation marks omitted).

Cravens did not “exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights” when he executed the Second Warrant. United States v. Davis, 131 S. Ct. at 2438 (citation omitted). Nishida did not begin searching Loera’s electronic media for child pornography until Judge Schneider had issued the Second Warrant. In doing so, Nishida reasonably and in good faith relied upon Judge Schneider’s determination that probable cause existed. As the Tenth Circuit explained in United States v. Nolan, 199 F.3d 1180, (10th Cir. 1999), “[w]here an officer acting with objective good faith obtains a search warrant from a detached and neutral magistrate and the executing officers act within its scope, there is nothing to deter.” 199 F.3d at 1184. Moreover, as explained previously, because of the volume of the child pornography evidence in this case, and because of the centrality of the child pornography to the United States’ case, the social costs of excluding such evidence would be high. The Court concludes, accordingly, that the good-faith balancing test weighs against excluding the child pornography evidence.

**IX. EVEN IF THE SECOND WARRANT CONTAINED AN INCURABLE DEFECT AND NISHIDA DID NOT EXECUTE THE SECOND WARRANT IN GOOD FAITH, THE AGENTS INEVITABLY WOULD HAVE DISCOVERED CHILD PORNOGRAPHY.**

Even if the Second Warrant contained an incurable defect and Nishida did not execute it in good faith, the agents inevitably would have discovered child pornography. The United States argues that all four of the United States v. Souza factors weigh in favor of finding inevitable

discovery. See Response at 18-19. Addressing the first factor, the United States argues that the First Warrant and the Second Warrant were obtained before Nishida began searching for child pornography. See Response at 18. Turning to the second factor, the United States contends that the strength of the probable cause showing was “undeniably high” when Nishida searched Loera’s CDs and laptop, because Cravens and Nishida had personally viewed child pornography on the CDs on November 20, 2012. Response at 18. Regarding the third factor, the United States says that Cravens obtained the Second Warrant and, had there been no Second Warrant, “there is no question that the FBI would have obtained a warrant authorizing a search for child pornography evidence once . . . Nishida found such evidence” during his search under the First Warrant. Response at 19. As to the fourth factor, the United States contends that Nishida and Cravens did not “jump the gun,” but instead had “complete confidence that probable cause existed to support the issuance of a search warrant,” because Nishida waited until he obtained the Second Warrant to conduct the search. Response at 19. The United States concludes its inevitable discovery argument by stating that, “if the Court finds the Second Warrant to have been invalid, the evidence obtained from the search authorized by the warrant should not be suppressed as it inevitably would have been lawfully discovered.” Response at 19.

Loera first argues that, without the Second Warrant, Nishida would have discovered child pornography only if he had exceeded the scope of the First Warrant by clicking on images and video files. See Supplement to Reply at 13-14 (citing Nix v. Williams; Walter v. United States, 447 U.S. at 654). Loera next contends that there is “no evidence” that Nishida or anyone else would have sought another search warrant if Nishida discovered child pornography on Loera’s laptop. Supplement to Reply at 13. Loera explains:

Nishida was not an affiant in seeking either of the two existing search warrants in this case. After allegedly finding child pornography on two CDs on

November 20, Nishida personally did not author or seek a search warrant to search the Dell laptop. Only after Cravens had conducted his unlawful warrantless search of the CDs for child pornography on November 27, did Cravens, not Nishida seek the second search warrant, which included the Dell laptop.

Supplement to Reply at 13. Loera also asserts that, had Nishida discovered child pornography on Loera's laptop while executing the First Warrant, Boady also would not have obtained a search warrant for child pornography, because Boady did not do so after Cravens told Boady that he found child pornography on Loera's CDs on November 20, 2012. See Supplement to Reply at 13. Loera concludes his inevitable discovery argument by contending that "[t]he historical facts fail to show with sufficient probability that Nishida would have sought a search warrant after finding child pornography on the laptop." Supplement to Reply at 13. The Court agrees with the United States.

Under the inevitable discovery exception, "illegally obtained evidence may be admitted if it 'ultimately or inevitably would have been discovered by lawful means.'" United States v. Christy, 739 F.3d at 540 (quoting Nix v. Williams, 467 U.S. at 444). "The government possesses the burden of proving by a preponderance of the evidence that the evidence at issue would have been discovered without the Fourth Amendment violation." United States v. Cunningham, 413 F.3d at 1203 (citation omitted). In United States v. Souza, the Tenth Circuit adopted four factors to determine "how likely it is that a warrant would have been issued and that the evidence would have been found pursuant to a warrant:"

1) the extent to which the warrant process has been completed at the time those seeking the warrant learn of the search; 2) the strength of the showing of probable cause at the time the search occurred; 3) whether a warrant ultimately was obtained, albeit after the illegal entry; and 4) evidence that law enforcement agents "jumped the gun" because they lacked confidence in their showing of probable cause and wanted to force the issue by creating a fait accompli.

223 F.3d at 1204 (citations omitted)(internal quotation marks omitted). Applying the first United

States v. Souza factor, the Tenth Circuit stated:

[T]he prerequisite to a consideration of the inevitable discovery exception in these cases, steps taken to obtain a warrant prior to the unlawful search, is present in this case. Special Agent Rowden took steps to alert his office that he would be coming back to prepare a warrant for the package and made sure that the affidavit form would be ready when he got back to his office. Also, the package was specifically placed on the floor behind Detective Sloan for the purpose of obtaining a warrant.

223 F.3d at 1205. Regarding the second factor, the Tenth Circuit stated:

[A]t the time the illegal search occurred, probable cause to believe the package contained contraband was extremely strong. The package itself contained several suspicious characteristics, including all of the openings on the box being heavily taped, the box having been sent through third party shipping, the sender having only used a first name, and the box being solid so that no side of it could be compressed. Moreover, the box was alerted to by a certified narcotics dog, which is itself sufficient to create probable cause.

223 F.3d at 1205-06. The Tenth Circuit noted that a sergeant eventually obtained a search warrant. See 223 F.3d at 1206. Regarding the third factor, the Tenth Circuit stated that, unlike “Cabassa, there is no question . . . concerning the inevitability of discovery of the evidence if the police had obtained a search warrant because the package was secured by the officers and there was no chance that it would not still be there when the warrant actually was issued.” 223 F.3d at 1206. The Tenth Circuit, thus, stated that, although it was

very reluctant to apply the inevitable discovery exception in situations where the government fails to obtain a search warrant and no exception to the warrant requirement exists, in this case the inevitability of discovery of the evidence convince[d] [it] that [the case before it was] one of those occasions when the doctrine should apply.

223 F.3d at 1206.

In United States v. Christy, the Court applied the four United States v. Souza factors and determined that the inevitable discovery exception applied. See 810 F. Supp. 2d at 127. Regarding the first factor -- the extent to which the warrant process had been completed at the

time those seeking the warrant learn of the search -- the Court stated:

The deputies did not take any steps to obtain a warrant before entering Christy's residence. The United States concedes that they did not attempt to obtain a warrant before entering Christy's residence. . . . This factor thus weighs against applying the inevitable discovery exception.

810 F. Supp. 2d at 1275 (citations omitted). As to the second factor -- the strength of the showing of probable cause at the time the search occurred -- the Court concluded:

The Court finds that [Investigator Carvo] had strong probable cause that Christy committed crimes. At the time of the search, Carvo believed he had probable cause for the California crime of unlawful sexual intercourse, because Christy and K.Y. exchanged naked pictures through electronic mail transmissions over the internet and then arranged a meeting in the middle of the night for K.Y. to run away with Christy.

. . . .

Because [the officer] knew that K.Y. and Christy were exchanging naked pictures, "the belief that there was a sexual relationship or sexual interest between the two was reasonable." Amended Memorandum Opinion and Order at 57. These circumstances are sufficient to form "a reasonable ground for belief of [Christy's] guilt," . . . for the California crime of unlawful sexual intercourse.

[The officer] also had strong probable cause for the federal crime of coercion or enticement. Carvo believed that he had probable cause for the federal crime of enticement or coercion, because of Christy's and K.Y.'s communications through the internet and electronic mail transmissions, because Christy sent K.Y. naked pictures of himself and solicited pictures of K.Y., which showed her breasts, and because cellular telephone evidence shows that Christy traveled across state lines to bring K.Y. to New Mexico.

. . . .

Because [the officer] knew that Christy and K.Y. communicated through electronic mail transmissions, that Christy sent K.Y. naked pictures of himself and solicited pictures of K.Y., because evidence showed that Christy traveled across state lines with K.Y., and because Carvo had strong probable cause that Christy committed the California crime of unlawful sexual intercourse, Carvo had "a reasonable ground for belief of [Christy's] guilt," . . . for the federal crime of coercion or enticement. Because Carvo had strong probable cause for the California crime of unlawful sexual intercourse and for the federal crime of enticement or coercion, this factor weighs in favor of application of the inevitable discovery doctrine.

810 F. Supp. 2d at 1276-78 (brackets in original)(citations omitted). Regarding the third factor, -- whether a warrant ultimately was obtained, albeit after the illegal entry -- the Court held:

The deputies “ultimately did obtain a warrant, albeit based in part on information retrieved” from Littlefield’s actions of peering through a crack in the blinds in Christy’s window, and from the deputies’ entry into Christy’s residence and subsequent interview of Christy. United States v. Cunningham, 413 F.3d at 1205. Although portions of the affidavits supporting the warrants were based on information the Court has found illegally obtained, the affidavits also included information from the California investigation. Although the Tenth Circuit appears to rely on illegally obtained information in its inevitable discovery analysis, the Court does not believe that it can do so. Carvo had strong probable cause that Christy committed California and federal crimes, and Carvo’s probable cause was based on his investigation, and not on any information he learned from the BCSO or from the Albuquerque FBI. . . . Because Carvo had strong probable cause for a California crime and a federal crime, based on information that he learned in his investigation, and not based on information he learned from the BCSO or from the Albuquerque FBI, Carvo would have obtained search warrants that were not based on illegally obtained information. Based upon Carvo’s belief that he had probable cause for both violations of California state law and violations of federal law, he would “have asked [BCSO] and/or -- either one -- the FBI to obtain a search warrant for [Christy’s] Albuquerque residence, vehicle, computers, cell phones, things of that nature.” . . . If the BCSO or Albuquerque FBI were not able to obtain a search warrant for these locations, Carvo would have written a federal search warrant himself and come to the District of New Mexico to seek the warrant with himself as the affiant. . . . Carvo is cross designated to acquire both state and federal search warrants. . . . This factor thus weighs in favor of application of the inevitable-discovery doctrine.

810 F. Supp. at 1278-79. As to the fourth factor -- the existence of evidence that the officers jumped the gun because they lacked confidence in their showing of probable cause and wanted to force the issue by creating a *fait accompli* -- the Court determined:

There is “no evidence that the officers ‘jumped the gun’ due to a lack of confidence about probable cause and out of a desire to force the issue.” United States v. Cunningham, 413 F.3d at 1205. The record indicates that the search occurred when it did because the deputies believed that they had exigent circumstances to enter Christy’s residence. This factor thus weighs in favor of application of the inevitable discovery doctrine.



810 F. Supp. 2d at 1279. Consequently, the Court applied the inevitable discovery doctrine. See 810 F. Supp. 2d at 1279.

On appeal, the Tenth Circuit affirmed the Court's decision. See 739 F.3d at 539-44. In an opinion that Judge Kelly authored, and Judges Hartz and Matheson joined, the Tenth Circuit began by addressing the four factors from United States v. Souza. See 739 F.3d at 541. The Tenth Circuit pointed out that the defendant only challenged the Court's ruling on factors two and four -- the strength of the probable cause showing when the unlawful search occurred and whether the officers "jumped the gun" to sidestep the warrant requirement. 739 F.3d at 541. Regarding the second factor -- the strength of the showing of probable cause at the time the unlawful search occurred -- the Tenth Circuit stated:

The district court found that Officer Carvo knew that K.Y. was a minor, there was a large age difference between her and Mr. Christy, the two exchanged sexually explicit pictures, and that Mr. Christy traveled across state lines with K.Y. . . . Given those factual findings, it is a reasonable inference that a sexual relationship existed between Mr. Christy and K.Y. Officer Carvo also knew that K.Y. was potentially suicidal, had left her depression medication behind, and ran away from home with Mr. Christy. . . . Based on that knowledge, Officer Carvo's belief that K.Y. was at risk for sexual victimization and assault was reasonable. Thus, Officer Carvo had reasonable grounds to believe that Mr. Christy engaged in sexual activity in violation of California law and coerced or enticed K.Y. to travel across state lines to engage in criminal sexual activity in violation of federal law. . . . The district court was correct in weighing this factor in favor of applying inevitable discovery.

United States v. Christy, 739 F.3d at 542. Analyzing the fourth factor -- evidence that the officers jumped the gun because they lacked confidence in their showing of probable cause and wanted to force the issue by creating a fait accompli -- the Tenth Circuit explained:

Mr. Christy argues that the deputies "jumped the gun" by forcing entry into his home due to their lack of confidence about probable cause. . . . Yet as the district court found, no evidence supports the theory that the deputies forced entry for that reason. . . . Instead, the deputies forced entry because they believed K.Y. was in danger. . . . Mr. Christy argues that the search was not in fact justified by exigent circumstances and points to the district court's conclusion that it was not. . . . But

that is beside the point. The record fully supports the reasonableness of the deputies' assessment of danger. The district court was correct in weighing this factor in favor of the government.

United States v. Christy, 739 F.3d at 543. The Tenth Circuit concluded, therefore, that the Court properly applied the United States v. Souza factors. See 739 F.3d at 542.

The Court concludes that the inevitable discovery applies. First, Cravens and Nishida did not take substantial steps to obtain a search warrant for child pornography before the contested November 27, 2012, searches occurred. Cravens only intended to obtain a search warrant -- but had not undertaken any formal steps to do so -- when he conducted the unlawful searches of Loera's CDs on November 27, 2012. Consequently, the first factor -- the extent to which the process for the Second Warrant had been completed at the time those seeking the warrant learn of the unlawful search -- weighs against finding inevitable discovery.

Second, the agents possessed strong probable cause for their search of Loera's media before Cravens' unlawful search on November 27, 2012. Both Cravens and Nishida each viewed at least two images of child pornography on Loera's CDs when they executed the First Warrant on November 20, 2012. Although Cravens and Nishida did not note any locations, filenames, or descriptions of the images they viewed, had Cravens known he was not permitted to search Loera's CDs on November 27, 2012, either he or Nishida likely would have been able to describe at least one of the images with sufficient particularity to establish probable cause. Accordingly, the second factor -- the strength of the showing of probable cause at the time the search occurred -- weighs in favor of finding inevitable discovery.

The agents ultimately obtained a warrant, albeit based in part on the information that Cravens obtained from his unlawful November 27, 2012, searches of Loera's CDs. This factor cuts slightly in favor of finding inevitable discovery. There is also no evidence that the agents

“jumped the gun” because of a lack of confidence about probable cause and out of a desire to force the issue. 223 F.3d at 1204. Instead, the record indicates that the November 27, 2012, search occurred when it did, because Cravens mistakenly believed that he could search Loera’s CDs to provide Judge Schneider a detailed description of one image of child pornography from each of the CDs. As a result, the Court concludes that, as in United States v. Souza, but for Cravens’ unlawful search on November 27, 2012, Nishida and Cravens would have obtained an untainted search warrant and the evidence in question would have been found. See 223 F.3d at 1205. The Court concludes, accordingly, that the inevitable discovery exception would apply even if the Second Warrant contained an incurable defect and Nishida did not act in good faith in executing it.

The Court may apply the inevitable discovery exception in this case despite there not being a second, independent investigation through which law enforcement could have obtained the child pornography evidence in this case. In United States v. Christy, the Tenth Circuit stated that no such requirement exists. See United States v. Christy, 739 F.3d at 540. In United States v. Christy, Judge Kelly explained:

In Cunningham and Souza we applied inevitable discovery to situations like the one here -- where there was “one line of investigation that would have led inevitably to the obtaining of a search warrant by independent lawful means but was halted prematurely by a search subsequently contended to be illegal.” Cunningham, 413 F.3d at 1204 n.1. In Cunningham, police searched the defendant’s home after getting his consent. Id. at 1202. The defendant later contested the search, claiming his consent was coerced. Id. We held that even if the search was illegal, the evidence was admissible because the officers “would have obtained a search warrant” if the search had not occurred. Id. at 1205. In Souza, police illegally opened a UPS package that contained drugs. 223 F.3d at 1200, 1202. We held the evidence admissible under inevitable discovery because the officers “would have obtained a warrant” had the illegal search not occurred. Id. at 1206. Thus, our case law does not require a second investigation when the first (and only) investigation would inevitably have discovered the contested evidence by lawful means.

....

Thus, lest there be any doubt, we reaffirm the notion that inevitable discovery requires only that the lawful means of discovery be “independent of the constitutional violation,” Larsen, 127 F.3d at 987, and conclude that a second investigation is not required.

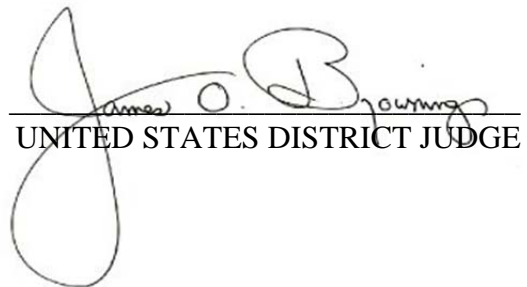
United States v. Christy, 739 F.3d at 540-41.

In this case, as in United States v. Cunningham, there was “one line of investigation that would have led inevitably to the obtaining of a search warrant by independent lawful means but was halted prematurely by a search subsequently contended to be illegal.” United States v. Cunningham, 413 F.3d at 1204 n.1. In United States v. Cunningham, the officers focused their investigation on two homes -- 1175 and 1179 East 76th Terrace -- and had drafted an affidavit to support a search warrant for one of the homes. See 413 F.3d at 1200-1201. The officers had sufficient probable cause to search either home. See 413 F.3d at 1201. Rather than running the risk that they would search the wrong home, however, the officers conducted surveillance of both homes. See 413 F.3d at 1201. While conducting surveillance, the officers obtained consent to search 1179 East 76th Terrace, and subsequently discovered evidence that incriminated the defendant. See 413 F.3d at 1201-1202. The Tenth Circuit found that, even if the consent was obtained unlawfully, the four United States v. Souza factors indicated that the officers would inevitably have discovered the evidence. See 413 F.3d at 1204-1205. It was, therefore, immaterial that there was no second, independent investigation through which law enforcement would have lawfully discovered the evidence. See 413 F.3d at 1204-1205.

As in United States v. Cunningham, Cravens and Nishida had sufficient probable cause to search Loera’s CDs before Cravens searched them on November 27, 2012. See 413 F.3d at 1201. Like the officers in United States v. Cunningham, who drafted a search warrant affidavit before the allegedly unlawful search occurred, Cravens intended to obtain a warrant to search

Loera's CDs before his unlawful search occurred. See 413 F.3d at 1200-1201. Like in United States v. Cunningham, where, had the officers not searched the defendant's residence pursuant to unlawfully obtained consent, they would have obtained the same evidence lawfully by executing a search warrant, the agents in this case, had Cravens not unlawfully searched Loera's CDs on November 27, 2012, would have obtained the same evidence by lawfully executing a search warrant. See 413 F.3d at 1204-1205. It is, therefore, immaterial that there was no second, independent investigation through which law enforcement would have lawfully discovered the child pornography evidence. The Court holds, accordingly, that the inevitable discovery exception applies.

**IT IS ORDERED** that Defendant Jason Loera's Motion to Suppress Evidence, filed March 7, 2014 (Doc. 35), is denied. The Court will, therefore, not exclude from trial the child pornography evidence discovered on the media items seized from Defendant Jason Loera's residence.



UNITED STATES DISTRICT JUDGE

*Counsel:*

Damon P. Martinez  
United States Attorney  
Dean S. Tuckman  
Cynthia Weisman  
Kristopher N. Houghton  
Assistant United States Attorneys  
United States Attorney's Office  
Albuquerque, New Mexico

*Attorneys for the Plaintiff*

Thomas M. Blog  
Santa Fe, New Mexico

--and--

David C. Serna  
David C. Serna Attorney at Law  
Albuquerque, New Mexico

*Attorneys for the Defendant*